SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

DIPLOMSKI RAD br. 1373

Analiza i usporedba sigurnosnih mehanizama u Internetu stvari

Filip Ptiček

Zagreb, lipanj 2021.

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Zagreb, 12. ožujka 2021.

DIPLOMSKI ZADATAK br. 1373

Pristupnik:	**Filip Ptiček (0036491837)**
Studij:	Informacijska i komunikacijska tehnologija
Profil:	Telekomunikacije i informatika
Mentor:	izv. prof. dr. sc. Marin Vuković

Zadatak: **Analiza i usporedba sigurnosnih mehanizama u Internetu stvari**

Opis zadatka:

Posljednjih godina razvoj bežičnih pristupnih mreža te energetski efikasnih ugradbenih računala ima za posljedicu pojavu malih uređaja koji nude mogućnosti kontrole, mjerenja i praćenja okoline. Jedan od izazova Interneta stvari je sigurnost i privatnost korisnika te njihovih podataka. Taj izazov je posebno naglašen zbog heterogenosti uređaja i protokola za komunikaciju potrebnih kod implementacije sustava. Vaš je zadatak istražiti i usporediti postojeće tehnologije i protokole za komunikaciju te zaštitu podataka u okolini Interneta stvari. Na temelju istraživanja potrebno je osmisliti i implementirati rješenje na kojem ćete analizirati protokole u smislu osiguravanja osnovnih sigurnosnih zahtjeva.

Rok za predaju rada: 28. lipnja 2021.

SADRŽAJ

1. Uvod

Internet stvari sve više obuhvaća našu okolinu i sadašnjicu. Pojavom brzih bežičnih pristupnih mreža te sve manjih i učinkovitijih uređaja se povezanost usadila u sve aspekte naših života. Pametni domovi, pametni gradovi i industrija 4.0 samo su neki od primjera gdje Internet stvari nalazi svoju primjenu. Povezanošću uređaja i krajnjih korisnika olakšavaju se razni dnevni procesi te se pokazuje prilika za pojavom novih koji prije nisu bili mogući. Iako se pojam Interneta stvari pojavio u zadnjih dvadeset godina, potreba za umrežavanjem uređaja datira od samih početka pojave Interneta.

Tako se prvi pametni uređaj povezan na mrežu našao u Sveučilištu Carnegie Mellon u Pensilvaniji, 1982. godine. Zbog tromosti i iritiranosti jednog studenta, prouzročenom praznim automatom za pića, on je odlučio spojiti automat na ARPANET, preteču javna mreža Internetu, kako bi mogao doznati trenutno stanje automata[1]. Iako taj postupak tada nije bio smatran revolucionarnom idejom, broj umreženih aparata danas ukazuje na suprotno.

Trend područja Interneta stvari je u brzom rastu te poprima sve veću primjenu u svim područjima socijalnog života i poslovnih procesa te je važno definirati i rastumačiti sigurnosne mehanizme vezane uz Internet stvari kako bi implementacijska rješenja krajnjim korisnicima pružala adekvatnu razinu sigurnosti i privatnosti.

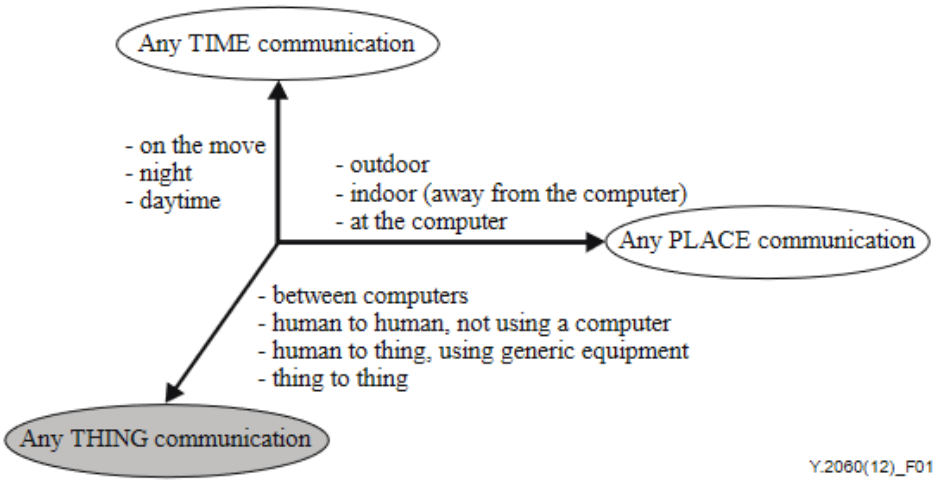
Ovaj rad primarno obrađuje sigurnosne mehanizme u Intenetu stvari uz glavni naglasak na informacijsku sigurnost, analizu i usporedbu sigurnosnih mehanizama protokola te implementaciju i sigurnosnu analizu sustava za praćenje tjelesne temperature.

U sljedećem poglavlju će se definirati pojam, referentni model, izazovi, područja primjene i trendovi u Internetu stvari. Treće poglavlje obrađuje zahtjeve vazane uz sigurnost i privatnost te sigurnosne propuste u Internetu stvari. U četvrtom poglavlju se kroz protokolni složaj Interneta stvari analiziraju i uspoređaju protokoli svakog sloja uz naglasak na sigurnosnim mehanizmima protokola. Peto poglavlje opisuje implementaciju sustava za prećenje tjelesne temperature, arhitekturu sustava, korištene razvojne alate i uređaje, opisuje rad sustava i analizu sigurnosti sustava. Konačno u zaključku...dopisati nakon napisanog zaključka.

2. Internet stvari

2.1. Definicija

The International Telecommunication Union(ITU-T) je specijalizirana agencija Ujedinjenih Naroda za informacijske i komunikacijske tehnologije. ITU-T definira Internet stvari kao globalnu infrastrukturu za informacijsko društvo, koja omogućava napredne usluge međusobnim povezivanjem (fizičkih i virtualnih) stvari na temelju postojećih i razvijajućih interoperabilnih informacijskih i komunikacijskih tehnologija. Iskorištavanjem identifikacije, prikupljanja podataka, obrade i komunikacijskih sposobnosti, Internet stvari u potpunosti upotrebljava mogućnosti povezanih stvari kako bi ponudio usluge za mnogo različitih primjena, uz osiguravanje sigurnosti i privatnosti. Sa šire perspektive, Internet stvari može biti percipiran kao vizija s tehnološkim i društvenim implikacijama[3]. Informacijske i komunikacijske tehnologije (ICT) pružaju komunikaciju u bilo koje vrijeme i na bilo kojem mjestu dok Internet stvari dodaje još jednu dimenziju gdje se radi o bilo kojoj stvari u komunikaciji. Te tri dimezije komunikacije su prikazane na sljedećoj slici.

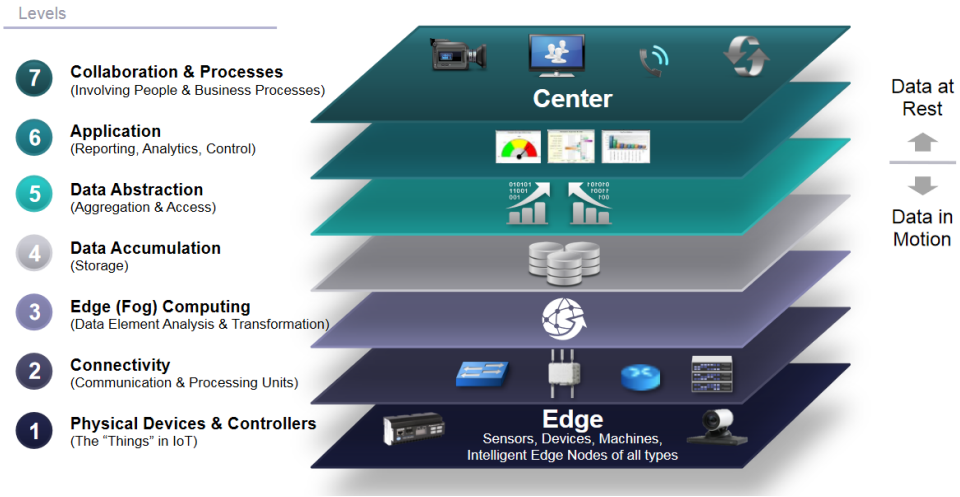


Slika 2.1: Nova dimenzija komunikacije predstavljena u Internetu stvari[3]

ITU-T također definira pojmove uređaja i stvari u kontekstu Interneta stvari. Uređaj je dio opreme s obaveznom mogučnošću komunikacije i neobaveznim mogućnostima opažanja, aktuacije te prikupljanja, pohrane i obrade podataka. Pojam stvari je definiran kao objekt u fizičkom svijetu (fizička stvar) ili u informacijskom svijetu (virtualna stvar) koja ima sposobnost da bude identificiran i integrirana u komunikacijsku mrežu. Fizičke stvari postoje u fizičkom svijetu i imaju sposobnosti biti opažene, aktuirane i povezane, a virtualne stvari potoje u informacijskom svijetu i imaju sposobnosti biti spremljene, obrađene i pristupljene. Neki od primjera fizičkih stvari su: okolina, industrijski roboti, priozvodi i električna oprema, dok primjeri virtualnih stvari su multimedijski sadržaji i programska podrška.

2.2. Referentni model

Ako promatramo Internet stvari kao jedan zaseban ekosustav potrebno je definirati referentni model prema kojem možemo opisati sve dijelove sustava i njegove zahtijeve. S obzirom na to da je Internet stvari pojam koji opisuje povezanost stvari, a ne i konkretan referentni model, od pojave samog pojma su se predlagani različiti modeli koji bi predstavljali cijeli spektar mogućnosti i zahtijeva Interneta stvari.



Slika 2.2: Cisco Internet stvari referentni model[4]

Ciscov referentni model Interneta stvari[4] definira višeslojni model od kojih svaki sloj definira terminologiju koja može biti standardizirana kako bi se stvorio globalni referentni okvir. Ovaj model ne definira lokalnost komponenata već opisuje zadatke koje svaki sloj obavlja kako bi se održala jednostavnost, omogućila skalabilnost i osigurala potpora. Model također definira funkcije koje su potrebne kako bi sustav Interneta

stvari bio kompletan. Na slici 2.2 je prikazan Ciscov Internet stvari referentni model i njegovi slojevi. Put podataka između slojeva je dvosmjeran, dok put kontrolnih informacija je s viših slojeva prema nižim slojevima. Kod promatranja je put informacija u obrnutom smjeru, od nižih slojeva prema višim.

2.2.1. Fizički uređaji i kontroleri

Referentni model počinje s prvim slojem: fizički uređaji i kontroleri koji mogu upravljati s više uređaja. Ovo je sloj koji opisuje stvari u kontekstu Interneta stvari i uključuje različiti raspon uređaja koji šalju i primaju informacije. Uređaji su različitih veličina, izgleda i namjene te potječu od različitih proizvođača. Kako bi se pojednostavila kompatibilnost referentni model općenito opisuje razinu obrade potrebne od uređaja. Neke od osnovnih sposobnosti uređaja uključuje: pretvorbu analognih u digitalne signale, generiranje podataka i mogućnost da se uređajem upravlja i šalju upiti.

2.2.2. Povezanost

Komunikacije i povezanost su sadržani u drugom sloju. Najvažnija mogućnost ovog sloja je sposobnost pouzdanog i pravovremenog prijenosa informacija. Time se definira prijenos između uređaja i mreže, između mreža te između mreže i računanja na rubu mreže (engl. *Edge Computing*) na trećem sloju. Jedan od cilja referentnog modela je da se sva komunikacija odvija putem postojećih mreža. Kako neki uređaji ne podržavaju IP protokol, potrebno je u mrežu uvesti prilaze (engl. *gateway*) koji će služiti kao posrednik između uređaja i ostatka mreže. Na ovom sloju se pojavljuje velika heterogenost komunikacijskih i pristupnih protokola koji uvelike ovise o željenoj namjeni uređaja prvog sloja. Ovaj sloj je usko povezan sa TCP/IP složajnim modelom koji sadrži protokole fizičkog sloja, sloja podatkovne poveznice te mrežnog, transportnog i aplikacijskog sloja.

2.2.3. Računarstvo na rubu mreže

Funckija trećeg sloja je vođena potrebom za pretvaranjem mrežnog podatkovnog prometa u informacije koje su prikladne za pohranu podataka i za obradu na višim slojevima. Treći sloj je zadužen za obradu podataka i njihovu transformaciju. Jedno od načela ovog referentnog sloja je da se obrada podataka odvija što je ranije moguće i što bliže rubu mreže kako bi se smanjila potreba za odvijanjem obrade velikog skupa podataka na udaljenom i centralnom mjestu. Obrada na trećem sloju obuhvaća razne

primjere poput: evaluacije, formatiranja, proširivanja, dekodiranja, redukcije i procjene značenja podataka.

2.2.4. Akumulacija podataka

Mrežni sustavi su izgrađeni za pouzdani prijenos podataka. Prije četvrtog sloja podaci su u stanju prijenosa. Takvi podaci proizlaze iz prvog i prolaze kroz drugi i treći sloj. Kako u nekim slučajevima ne postoji potreba za trenutnom obradom tih podataka, oni dolaze do četvrtog sloja gdje se podaci spremaju u memoriju. Na ovom sloju su podaci trajni i nepromjenjivi te spremni za posluživanje višim slojevima referentnog modela. Četvrti sloj određuje jesu li podaci važni za više slojeve, ako jesu, potrebno je osigurati načine posluživanja tih podataka zahtijevima viših slojeva. Određuje je li potrebno da podaci budu trajni, tj. treba li podatke spremiti na trajnu ili ih je dovoljno spremiti u radnu memoriju za kratkoročnu upotrebu. Kakav tip pohrane podataka je potreban: datotečni sustav, distribuirani datotečni sustav ili neki oblik baze podataka. Na koji način je organizirano spremanje podataka te je li potrebno podatke spojiti, preračunati i agregirati s prethodno spremljenim podacima. Ukratko, zadaća četvrtog sloja je da podatke bazirane na događajima pretvori u podatke nad kojima se rade upiti za potrebe viših slojeva.

2.2.5. Apstrakcija podataka

Funkcije apstrakcije podataka petog sloja su fokusirane na prikazivanje podataka i njihovu pohranu na način koji dozvoljava razvoj jednostavnijih, brzih aplikacija. Kako u modelu Interneta stvari postoji više uređaja koji generiraju podatke tako postoje različiti razlozi zašto podaci nisu prisutni na istom podatkovnom spremištu: previše podataka za spremanje na jedno mjesto, uređaji su geografski odvojeni, a obrada je optimizirana lokalno, postoji potreba za različitim načinima obrade podataka te se koriste različiti načini akumulacije podataka. Zbog tih razloga peti sloj je zadužen za različite vrste obrade poput ujednačavanja različitih formata podataka iz različitih izvora, osiguravajući dosljednu semantiku podataka kroz različite izvore, potvrda o potpunosti podataka šestom aplikacijskom sloju, zaštita podataka korištenjem autorizacijskih i autentifikacijskih mehanizama te normaliziranje i indeksiranje podataka za brz pristup od strane aplikacija.

2.2.6. Aplikacije

Na šestom sloju se nalazi aplikacijski sloj koji obavlja interpretaciju informacija. Ovaj referentni model ne definira strogo aplikaciju. Aplikacije se razlikuju na temelju različitih tržišta, prirode podataka i poslovnih potreba. Primjeri različitih potreba su aplikacije koje su usredotočene na promatranje i prikupljenje podataka, neke aplikacije se koriste za kontrolu uređaja dok neke kombiniraju podatke s uređaja i drugih izvora. Aplikacije predstavljaju različite modele upotrebe, razvojnih obrazaca, korištene razvojne programske podrške te krajnje kompleksnosti upotrebe. Neki primjeri aplikacija su povezane sa specijaliziranim industrijskim riješenjima, mobilne aplikacije koje obavljaju jednostavne interakcije, izrada izvješća povezanih uz poslovne procese, analitičke aplikacije koje obrađuju i interpretiraju podatke važne za poslovne odluke i aplikacije za upravljanje i kontroliranje ostatkom sustava. Ako su prijašnji slojevi dizajnirani pravilno to će utjecati na količinu posla koje sama aplikacija mora raditi dok će to zauzvrat olakšati procese na sedmom sloju.

2.2.7. Suradnja i procesi

Zadnji sedmi sloj referentnog modela uključuje ljude i poslovne procese. Ljudi koriste aplikacije i pridružene podatke za svoje specifične potrebe. Često, više ljudi koriste iste aplikacije za različite svrhe. Tako cilj cijelog sustava Interneta stvari nije sama aplikacija nego kao ispomoć u radu ljudi. Aplikacije pomažu ljudima kako bi mogli obavljati različite poslovne procese uz odgovarajuće podatke u pravo vrijeme. Poslovni procesi nerijetko uključuju rad i komunikaciju između više ljudi. Ljudi surađuju i komuniciraju međusobno kako bi potpora Interneta stvari bila korisna. Zato ti procesi zahtijevaju više koraka koji obuhvaća više aplikacija. Stoga zadnji sloj predstavlja višu razinu od jedne aplikacije.

2.3. Izazovi

Internet stvari kao pojam i skup tehnologija donosi i određene izazove. S obzirom na to da je Internet stvari široko područje, koje ima različita područja primjene, tako su i izazovi s kojima se susreće kod razvoja, planiranja i održavanja sustava brojni. Korištenjem pravilnih oblikovnih obrazaca postižu se bolja svojstva sustava te se olakšava daljnje održavanje i korištenje. U nastavku su nabrojani i opisani neki od izazova koji se pojavljuju u sustavima Interneta stvari.

2.3.1. Heterogenost

Heterogenost se pojavljuje na svakom implementacijskom koraku Internet stvari sustava. Heterogenost uređaja, komunikacijskih, pristupnih i transportnih protokola, programske podrške i samih potreba korisnika. Naravno ovakva vrsta heterogenosti se javlja zbog različitih potreba i radnih procesa. Uređaji koji se koriste nude različite potrebe u vidu veličine, potrebe za vanjskim napajanjem te dometu komunikacijskih kanala, radilo se o žičanoj ili bežičnoj komunikaciji. Protokoli koji vrše komunikaciju između uređaja i nekog oblika prilaza također ovise o tim potrebama, radilo se o potrebi za velikim transportnim brzinama ili o korištenje radiokomunikacije niske snage kako bi se očuvala energija uređaja. Također treba li komunikacija biti pouzdana i sigurna ovisi o korištenju različitih transportnih protokola te kriptografskih algoritama. Na sve navedeno utječu i sami radni procesi i potrebe korisnika. Ovisno o tome sami sustavi su osmišljeni za potrebe korisnika.

Heterogenost koja se javila u prvim razdobljima razvoja Interneta svari je povezano s nepostojanjem standardizacije i interoperabilnosti uređaja i postojećih programskih platformi. Tako se na primjeru pametnih domova pojavili različiti pametni uređaji od kojih je svaki zahtijevao vlastitu programsku platformu za upravljanje zbog nepostojanja interoperabilnosti s centralnim upravljačkim platformama. Kroz vrijeme su se pojavili zajednički napori proizvođača i različitih standardizacijskih tijela da se ovisno o području primjene Interneta stvari sustava postigne standardizacija komunikacijskih protokola i semantike informacija kako bi se postigla bolja interoperabilnost.

2.3.2. Raspodijeljenost

Kako u sustavima Interneta stvari sudjeluju različiti uređaji različitih prostornih lokacija tako se javlja i potreba za raspodijeljenosti sustava. Uređaji mogu biti mobilni što uvelike utječe na način pristupa kraljnjim programskim platformama s kojima uređaji komuniciraju. Od dovođenja uređaja u sustava, upravljanja uređaja, promatranja uređaja i samih aplikacija preko kojih se ti postupci provode se odvijaju raspodijeljenim putem. U nekim sustavima broj sudionika dostiže veliku brojku te je kod takvih sustava važno da se paralelno i konkurentno mogu odvajati aktivnosti. Otpornost na kvar je još jedan od zahtijeva koji prati raspodijeljene sustave kako bi se omogućo nesmetan rad sustava. Kod ispada i kvarova posljedice koje sustav Interneta stvari može imati na vanjski svijet je velik. Posebice u primjerima gdje se nadzire neki kritični sustavi poput industrijskih postrojenja. Također u pametnim domovima gdje različiti kućanski aparati su pretvoreni u pametne uređaje, kvarom poslužitelja mogu postati neupotrebljivi

te je važno da postoji redudantnost servisa s kojima uređaji komuniciraju.

2.3.3. Sigurnost

Sigurnost informacija i samih sustava je važan aspekt Interneta stvari u kojem sve više uređaja oko nas postaje umreženo. Problemi koji se javljaju su povezani s pokušajem brzog razvoja riješenja zbog konkurentnosti na tržištu, stavljanje u prvobitni plan funkcionalnosti sustava te dostupnosti prema korisnicima što stavlja sigurnost tih sustava u drugi plan. Kako mnogi uređaji i cjelokupni sustavi uvelike imaju kritične zadatke, poput medicinskih uređaja ili automobila, kompromitacija istih zbog sigurnosnih propusta može imati negativne posljedice. Također neki od primjera napada na sustave nije kako bi se napravila šteta sustavu, već za iskorištavanje procesne snage sustava u botnetovima. Sigurnosni propusti se mogu pojaviti na svakom dijelu sustava: uređaja, komunikacijskih kanala, poslužitelja, baza podataka i korisničkih sučelja. Neki od najvažnijih sigurnosnih zahtijeva na koje treba obratiti pozornost tijekom razvoja sustava Interneta stvari su obrađeni u trećem poglavlju.

2.3.4. Privatnost

Privatnost je uz sigurnost izazov s kojim se susreću mnogi sustavi Interneta stvari. Pametni uređaji koji se nalaze u našoj blizini imaju mogućnosti pratiti i bilježiti podatke o nama i našoj okolini. Kako korisnici priključuju sve više i više uređaja to je količina prikupljenih podataka veća, čime i povreda privatnosti može imati negativne posljedice na korisnika. Povrede te privatnosti mogu dolaziti u različtim oblicima. Od osobnih informacija koje mogu detaljno identificirati korisnika daju mogućnost napada u obliku krađe identiteta, medicinskih podataka ili pristupnih lozinki različitim servisima do kompromitacije sigurnosnih kamera što dozvoljava napadačima izravno praćenje korisnika. Privatnost podataka koji nisu isključivo vezani uz krajnje korisnike su i podaci pravnih osoba gdje može doći do narušavanja poslovnih tajni, autentifikacijskih i autorizacijskih podataka za razne servise i sigurnosne sustave. Kako pristupiti zaštiti privatnosti je usko povezano sa sigurnošću sustava te je obrađeno u trećem poglavlju.

2.3.5. Integracija

Nove tehnologije donose i nove integracijske probleme sa sobom. U slučaju Interneta stvari ovaj izazov je veći zbog heterogenosti svih dijelova koji čine sustave. U

slučaju heterogenosti sloja podatkovne poveznice i količine različitih protokola koji se koriste postoji problem uvođenja novih prijamnika i prilaza za te uređaje. Radi li se o niskofrekventnim riješenjima poput NFC-a ili protokolima poput ZigBee postoji potreba korištenja posebnih čitača ili prijamnika dok se taj problem ne pojavljuje kod WiFi protokola čija pristupna točka već postoji u većini domova. Nakon toga dolazimo do komunikacijske integracije između uređaja i poslužitelja, tj. programskih platformi. Na koji način će se odvijati prijenos podatka, kako će ti podaci biti organizirani te semantičko značenje tih istih podataka. Početkom razvoja riješenja Interneta stvari prvobitno su svi sustavi imali vlastite pristupne aplikacije. S pojavom želje za automatizacijom i međusobnom komunikacijom između uređaja različitih proizvođača počele su se razvijati platforme koje omogućuju interoperabilnost među sustavima te mogućnost upravljanja i praćenja uređaja putem jedne pristupne aplikacije. Kroz razvoj tih platformi proizvođači su počeli integrirati nove i postojeće uređaje da budu kompatibilni s njima.

2.4. Područja primjene

Internet stvari je širok u svojem području primjena. U današnjem svijetu postaje sve prisutnije u svakom aspektu života ljudi i taj trend će se nastaviti. Od naših domova do industrijskih postrojenja Internetu stvari omogućava pojednostavljenje naših života i poslovnih procesa. U nastavku su navedeni neke od glavnih područja primjene Interneta stvari i riješenja koja se koriste u tim područjima:

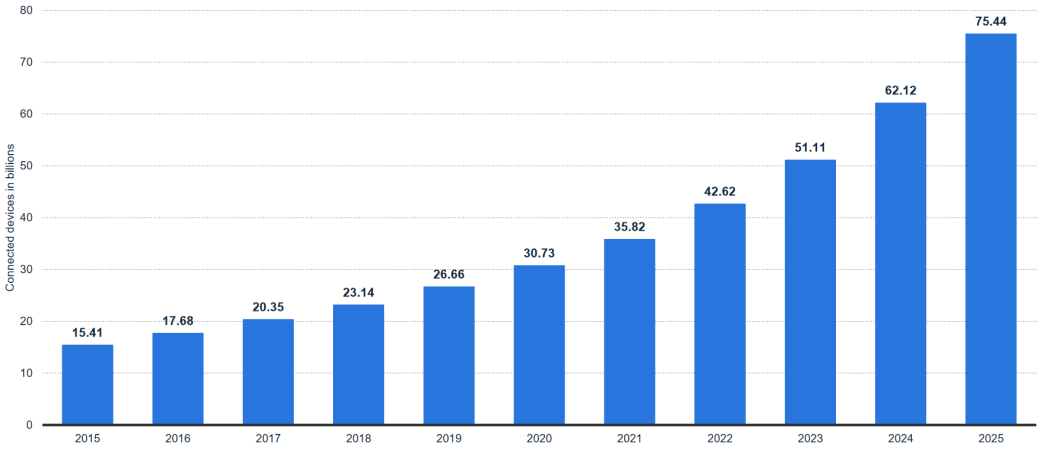
- Pametni dom
    - Pametna rasvjeta
    - Pametni kućanski aparati
    - Detekcija uljeza
    - Upravljanje energijom
- Pametni grad
    - Pametni parking
    - Upravljanje otpadom
    - Pametna rasvjeta
    - Reagiranje na hitne slučajeve
- Okoliš
    - Praćanje vremena

        - Praćenje zagađenja zraka
        - Praćenje zagađenja bukom
        - Detekcija požara
    - Prodaja
        - Upravljanje inventarom
        - Pametni automati za prodaju
        - Pametne blagajne
        - Pametno plaćanje
    - Logistika
        - Praćenje flote vozila
        - Praćenje pošiljaka
        - Dijagnostika vozila na daljinu
        - Generiranje i vremensko raspoređivanje voznih ruta
    - Industrija
        - Dijagnostika strojeva
        - Praćenje dijelova proizvodnje
        - Automatizacija proizvodnih procesa
    - Poljoprivreda
        - Pametno navodnjavanje
        - Praćenje usjeva
        - Automatizacija obrađivanja

2.5. Trendovi

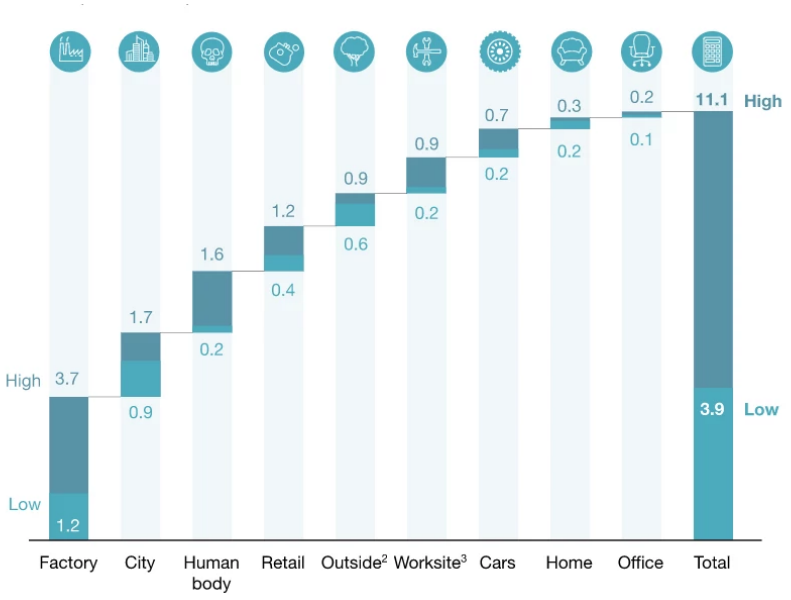
Internet svari se pojavio kao zamisao za daljnju budućnost, ali je već danas sadašnjost u socijalnim i proizvođačkim aspektima svijeta. To može biti pripisano pristupačnijim, procesorski bržim, energetski učinkovitijim te sve manjim uređajima za kojima raste potražnja integracije takvih riješenja u različita područja koja također kroz vrijeme postaju sve raznovrsnija. Trenutni broj umreženih Internet stvari uređaja doseže brojku od 35.82 bilijuna uređaja. Pojavom novih tehnologija poput 5G mreža, koje dozvoljavaju još veće brzine i smanjeno vrijeme odaziva, taj trend će kroz godine još više rasti te su neke od projekcija za godinu 2025. u iznosu od 75.44 bilijuna uređaja[6].

Trend broja umreženih Internet stvari uređaja između 2015. godine i predikcije do 2025. godine su prikazane na sljedećoj slici.



Slika 2.3: Broj povezanih Internet stvari uređaja[6]

Ako promatramo porast broja umreženih Internet stvari uređaj možemo zaključiti da s time postoji i veliki tržišni potencijal. Korisnika je sve više te je procjenjeno da svaki posjeduje prosječno četiri Internet stvari uređaja te da se u svijetu svake sekunde spoji novih 127 uređaja. Tako su i procjene za ekonomski utjecaj Interneta stvari na tržište između 3.9 i 11.1 bilijuna američkih dolar kroz različita područja primjene uključujući tvornice, gradove, domove i prodaju[28]. Na sljedećoj slici su prikazane niske i visoke predikcije za ekonomski utjecaj Interneta stvari za 2025. godinu.



Slika 2.4: Potencijalni ekonomski utjecaj kroz različita područja primjene za 2025. godinu. u bilijunima američkih dolara[28]

3. Sigurnost u Internetu stvari

3.1. Zahtjevi vezani uz sigurnost i privatnost

Važnost sigurnosti i privatnosti je nezamjenjiva. Ta važnost se posebice očituje u sustavima Interneta stvari gdje je ponekad veći naglasak stavljen na funkcionalnost što stavlja sigurnosne zahtijeve u drugi plan. Jednostavni uređaji s malo procesorske snage imaju problema s obavljanjem zahtijevnijih kriptografskih algoritama te je studija iz 2019. godine utvrdila da od 56 milijuna ispitanih uređaja, 91.5% razmjene podataka je bilo nešifrirano[23]. Nedostatak iskustva u području razvoja Interneta stvari također utječe na slabu sigurnost uređaja jer se ponekad kod planiranja ne utvrde svi mogući sigurnosni propusti te zahtijevi koji su vezani uz sigurnost i privatnost. Ti zahtijevi su ključan dio očuvanja sigurnosti cijelokupnog sustava i privatnosti samih korisnika. Sigurnosni zahtjevi vezani uz sigurnost i privatnost su sljedeći[25]:

Tajnost: informacija nije dostupna ili je izložena neovlaštenim osobama, entitetima ili procesima.

Cjelovitost: točnost i potpunost informacije.

Raspoloživost: informacija je dostupna na zahtjev i omogućeno je njeno korištenje od strane ovlaštenih osoba, entiteta ili procesa.

Vjerodostojnost: osoba, entitet ili proces je zaista onaj kojim se predstavlja.

Odgovornost: obveza izvještavanja o aktivnostima i preuzimanja odgovornosti za njih.

Neporicanje: sposobnost dokazivanja događaja ili aktivnosti i osoba, entiteta ili procesa koji su ih pokrenuli ili u njima sudjelovali.

Pouzdanost: konzistentno ponašanje i rezultati.

3.2. Sigurnosni propusti

The Open Web Application Security Project® (OWASP) je neprofitna organizacija čiji je cilj napredak i poboljšanje računalne sigurnosti informacijskih sustava. OWASP kroz svoje projekte otvorenog koda vođenih putem razvojne zajednice radi na poboljšanju sigurnosti Interneta.

OWASP Internet of Things Project je projekt osmišljen kako bi pomogao proizvođačima, programerima i potrošačima bolji uvid i razumijevanje u sigurnosne probleme vezane uz Internet stvari. Na taj način korisnici u bilo kojem dijelu razvojnog procesa mogu donositi bolje odluke kod razvoja, postavljanja i pristupanja tehnologijama Interneta stvari[9]. 2018. godine izlazi *OWASP IoT Top 10* lista koja reprezentira deset najčešćih ranjivosti Internet stvari sustava. Svih deset sigurnosnih ranjivosti su navedeni u nastavku uz opis sigurnosnih praksi koje bi trebale spriječiti te ranjivosti i sigurnosne propuste.

3.2.1. Slabe, pogodljive ili tvrdo kodirane lozinke

Prvi navedeni sigurnosni problemi kod Internet stvari sustava su vezni uz lozinke. Da bi se uređaju moglo pristupiti i naknadno ga konfigurirati, uređaji dolaze s korisničkim računima koji služe korisnicima kako bi ih mogli upariti sa željenim sustavom ili kako bi proizvođač mogao upravljati uređajem u slučaju pomoći korisnicima ili kod ažuriranja uređaja. Za pristup tom korisničkom računu uređaja je potrebna lozinka koju krajnji korisnik kod prve upotrebe treba postaviti. Navike korisnika su većinom da iskoriste njima dobro poznatu lozinku koju koriste i za svoje druge korisničke račune. Ako napadač dobije pristup jednoj njihovoj lozinci ima i pristup ostalim računima. Na taj način se pristup korištenim uređajima koji imaju isto korisničko ime ili e-mail adresu i lozinku uvelike olakšava. Korisnici imaju i naviku koristiti slabe lozinke koje su vrlo česte i jako lako pamtljive. Tako su neke od najčešće korištenih lozinka jednostavni nizovi numeričkih znakova ili nizovi znakova na tipkovnici poput: 123456, 123456789, qwerty, ili sam engleski prijevod lozinke (engl. *password*)[27]. Napadi na lozinke se provode putem takozvanih *brute force* napada. Kako je procesna snaga današnjih računala dosegla vrlo visoke brzine računanja, tako se jednostavne i kratke lozinke mogu pogoditi u vrlo kratkom vremenu.

Ovakvi propusti ne zaobilaze ni proizvođače samih sustava i uređaja. Kod proizvodnje proizvođači na uređaje postavljaju iste lozinke za sve uređaje kako bi kod testiranja ispravnosti lakše pristupili istima. Jedan od najboljih pokazatelja takvog

pristupa su usmjerivači/modemi telekom operatera za pristup Internetu koji imaju postavljenu istu zadanu lozinku i korisničko ime poput "admin" ili "user" koju krajnji korisnici uređaja nikada ne promjene. Problem se također pojavljuje i u tvrdo kodiranim (engl. *hard coded*) lozinkama. Proizvođači postave takve lozinke na uređaje kako bi se uređaji mogli nesmetano povezati s vanjskim servisima, kako bi se proizvođači povezali na uređaj zbog otklanjanja pogrešaka ili kao način za vanjsko upravljanje uređajim. Ako napadač ima fizički pristup uređaju on može skenirati memoriju i pomoću raznih alata pronači lozinku spremljenu na samom uređaju. A kako proizvođači najvjerojatnije koriste istu lozinku za sve iste modele uređaja, napadač ima lak način za pristup i ostalim istim uređajima.

Kako bi se spriječila ova vrsta ranjivosti neki od sigurnosnih mjera koji bi se trebali pratiti su sljedeći. Korisnici bi kod prve upotrebe uređaja trebali promijeniti zadanu lozinku koristeći duge, kompleksne i jedinstvene nizove znakova. Najjednostavniji način za postići te zahtjeve je korištenjem upravitelja lozinkama. Oni daju mogućnost generiranja lozinki uz mogućnost spremanja istih bez potrebe da korisnik mora pamtiti sve jedinstvene i duge lozinke. Što se tiče zahtijeva sa strane prozivođača, oni bi trebali razriješiti bolje načine upravljanja uređajima kako bi se izbjeglo korištenje istih ili čak tvrdo kodiranih lozinka za pristup uređaju ili vanjskim servisima. Također bi proizvođači trebali upozoriti korisnika kod uspostave uređaja da promijeni zadanu lozinku.

3.2.2. Nesigurne mrežne usluge

Internet stvari uređaji koriste razne mrežne usluge kako bi mogli komunicirati s vanjskim servisima. Kako je moguće pristupiti tim uređajima putem Interneta potrebno je pravilno osigurati sigurnost tih mrežnih usluga koje se izvršavaju. Neautoriziran pristup preko usluga iskorištavajući zadane lozinke, otvorene mrežne priključke te nepravilno podešeni vatrozidi dozvoljavaju napadaču da dobije pristup uređajima i poslužiteljima. Takvi napadi dozvoljavaju izvršavanje malicioznog koda, iskorištavanje uređaja za botnet, krađu podataka ili onesposobljavanje sustava.

Neki od sigurnosnih mjera koje se mogu poduzeti za osiguravanje mrežnih usluga su:

- korištenje zasebne lokalne mreže za sve pametne uređaje,
- spajati uređaje na isključivo sigurne mreže,
- instaliranje regularnih softverskih ažuriranja,
- isključivanje svih usluga koje pružaju vanjski pristup uređaju,

- isključivanje nepotrebnih mrežnih priključaka i usluga,
- isključivo korištenje protokola koji koriste šifriranje.

3.2.3. Nesigurna sučelja ekosustava

Nesigurna web sučelja, pozadinski API-jevi, servisi u oblaku i mobilna sučelja, koja dozvoljavaju komunikaciju i interakciju s uređajem, čine sveukupni ekosustav Interneta stvari. Kompromitacija bilo kojeg dijela sustava može uzrokovati i kompromitaciju cijelokupnog sustava. Ranjivost kod načina autorizacije i autentifikacije između uređaja i poslužitelja ili korisnika mobilnih i web aplikacija i poslužitelja su jedan od vektora napada na sustav. Također nedostatak ili korištenje slabog šifriranja kod komunikacije može uzrokovati da napadač presretne i iskoristi sakupljene informacije za napad. Nedostatak pravilnog filtriranja ulazno/izlaznih podataka može dovesti do napada poput SQL injekcije. Još jedan projekt OWASP organizacije je *OWASP Top 10 Web Application Security Risks* koji nudi popis najčešćih ranjivosti za web i mobilne aplikacije. Nesigurna sučelja ekosustava imaju direktnu poveznicu s tim ranjivostima koje su:

- injekcije (SQL, NoSQL, OS, LDAP),
- neispravna autentifikacija,
- izlaganje osjetljivih podataka,
- XML External Entities(XXE) napadi,
- neispravna autorizacijska kontrola,
- pogrešna konfiguracija servisa,
- Cross-Site Scripting(XSS),
- nesigurna deserijalizacija podataka,
- korištenje bibilioteka i komponenta s poznatim sigurnosnim ranjivostima,
- nedovoljno korištenje logova i praćenja sustava.[7]

Pravilno podešavanje autorizacije i autentifikacije korisnika, ali i uređaja je najvažniji način osiguravanja raznih sučelja ekosustava. Filtriranje ulaznih i izlaznih podataka spriječava napade injekcijom, pravilno podešavanje poslužitelja da koriste kriptografske algoritme za sve servise kako bi osigurali privatnu i sigurnu komunikaciju. Kroz cijeli ekosustav je potrebna i uspostava logiranja i praćenja sustava kako bi se na vrijeme otkrila nepravilna ponašanja unutar samog sustava.

3.2.4. Nedostatak mehanizama za sigurnosna ažuriranja

Kroz vrijeme, za programska rješenja koja se trenutno koriste na uređaju će se pronači ranjivosti. Kako bi se na vrijeme i jednostavnim putem mogli spriječiti napadi koji iskorištavaju te ranjivosti potrebna su nam softverska ažuriranja, kao i ažuriranja samog ugrađenog programa (engl. *firmware*) uređaja. Ako ne postoji način kojim dovodimo takva sigurnosna ažuriranja na uređaj postoji rizik za kompromitacijom uređaja. Također ako su i implementirani načini sigurnosnih ažuriranja, potrebno je pridodati pažnju na način te implementacije ažuriranja. Ako se ne provjeravaju digitalni potpisi izvora ažuriranja, moguće je na uređaj poslati maliciozno ažuriranje koje će kompromitirati uređaj. Potrebno je i koristiti sigurne načine prijenosa tih ažuriranja poput šifriranja upotrebljavanog komunikacijskog kanala.

Trenutnim trendom brzog razvoja novih uređaja, prozivođači često ne daju dovoljno dugi period sigurnosnih ažuriranja. Tako će se desiti da proizvod nakon manje od dvije godine prestane dobivati ažuriranja te će pasti odluka na korisnika o tome hoće li kupiti novi uređaj ili riskirati kompromitaciju trenutnog. Najbolji pokazatelj toga su pametni telefoni od kojih većina tijekom svog perioda upotrebe dobije samo nekoliko sigurnosnih ažuriranja prije nego bude depricirana od strane prozivođača.

Kako bi se uređaji zaštili od budućih napada zbog novootkrivenih sigrunosnih propusta potrebno je pružati korisnicima uređaja nuditi dugotrajna i česta sigurnosna ažuriranja. Prijenos ažuriranja je neophodno prenositi putem sigurnih komunikacijskih kanal koji su šifrirani. Ažuriranjima koja su dostigla na uređaj je potrebno validirati izvor, provjeriti odgovara li digitalni potpis izvoru od kojeg bi trebalo stići ažuriranje te je potrebno i validirati samo ažuriranje kako bi se izbjeglo moguće umetanje malicioznog koda.

3.2.5. Upotreba nesigurnih ili zastarijelih komponenti

Nadovezano na nedostatak mehanizama za sigurnosno ažuriranje, peta po redu od sigurnosnih propusta je upotreba nesigurnih ili zastarijelih komponenti. Mnogi sustavi Interneta stvari kao dio svojeg programskog riješenja sadrže otvoreni kod koji održava zajednica koja nije direktno povezana s proizvođačem. Kada se otkrije ranjivost na nekom od korištenih otvorenih rješenja proizvođač ili čeka na sigurnosnu zakrpu, ili u najboljem slučaju će sam riješiti sigurnosni propust te ga javno objaviti kako bi doprinjeo razvoju otvorenog rješenja. Nakon što sigurnosna zakrpa bude razvijena potrebno je ažurirati sve uređaje ili dijelove sustava koji su ugroženi od tog sigurnosnog propust.

Ako govorimo o Internetu stvari u proizvođačkoj industriji, takozvanoj Industriji

4.0, upotreba zastarijele programske podrške, koja je potrebna zbog jako specifičnih uređaja za prozivodnju, čija zadnja verzija zna datirati i više od deset godina nije rijetka. Uvođenjem takvih uređaja u sustave Interneta stvari također utječe na sigurnost i integritet cijelokupnog sustava te ugrožavanje jednog uređaja može dovesti do napada na cijelog lanca opskrbe. Kod upotrebe gotovih proizvoda poput senzora, videokamera ili pametne rasvijete te integracijom istih u postojeći sustav također treba obratiti pozornost na dostupnost sigurnosnih ažuriranja te stanja uređaja kojeg proizvođač još uvijek nudi sigurnosnu podršku.

Kod planiranja razvoja Interneta stvari sustava potrebno je uzeti u obzir trenutno, a i buduće stanje razvojne i sigurnosne podrške vanjske programske potpore i komponenti sustava. Najbolji način za spriječavanje sigurnosnih propusta je korištenje vlastito razvijene programske potpore ili korištenje dobro podržanih vanjskih biblioteka otvorenog koda s jakom i aktivnom razvojnom zajednicom. Uporeba zastarijelih uređaja bez sigurnosne podrške proizvođača ili potporom koja uskoro dotiže krajnji period (engl. *end of life*) je potrebno izbjegavati. Nakon puštanja sustava u produkciju nadziranje i praćenje vijesti vezanih uz sigurnosne propuste upotrebljenih komponenti i programske podrške je važno kako bi se na vrijeme moglo spriječiti kompromitacija sustava. Sve ovo nije moguće ako bilo koji dio ustava nema implementirane mehanizme za sigurnosna ažuriranja. Ako neka od komponenti dostigne svoj krajnji period ažuriranja potrebno je tu komponentu ukloniti i zamijeniti ju drugom čija sigurnosna ažuriranja još uvijek su podržana.

3.2.6. Nedovoljna zaštita privatnosti

Uloga Interneta stvari je djelom prikupljanje različitih podataka i mjerenja. Neki od tih podataka su osobne prirode za korisnika poput: medicinskih podataka ili zvukovnih i video zapisa. Kompromitacija takvih privatnih podataka može negativno utjecati na sigurnost korisnika. Prostor na kojem se privatnost korisnika može narušiti je od samog uređaja koji prikuplja podatke, do komunikacijskih kanala preko kojih se podaci šalju do samih krajnjih servisa koji primaju i obrađuju te podatke, a zatim ih spremaju u baze podataka na poslužiteljma. Nedovoljna zaštita privatnosti je zapravo rezultat svih ostalih nabrojanih sigurnosnih ranjivosti nabrojanih u ovom odjeljku.

Za očuvanje privatnosti korisnika i načine obrade podataka korisnika u Europskoj uniji postoji uredba donešena od strane Europske unije pod nazivom *Opća uredba o zaštiti podataka(GDPR) (EU) 2016/679*[5]. Cilj uredbe je omogućiti građanima Europske unije veću kontrolu i uvid u podatke koji se prikupljaju. Na taj način građani mogu

tražiti brisanje svojih podataka i povećava se odgovornost pravnih osoba koje te podatke prikupljaju. Odgovornost se postiže mogućim nametnutim sankcijama, ako se utvrdi povreda podataka građana. Prikupljanje podataka je moguće uz izrazitu privolu građana korisnika čime se zabranjuje bilo kakvo prikupljanje podataka bez pristanka.

Šifriranje komunikacijskih kanal nekada ne osigurava i privatnost korisnika. Kako bi pametni uređaji mogli komunicirati s krajnjim poslužiteljima, koji mogu mijenjati svoju odredišnu adresu, koriste se domenska imena. Za razlučivanje tih adresa u brojčanje IP adrese koristi se protokol DNS(engl. *Domain Name System*). Kada uređaji rade DNS upite u sadržaju upita se prikazuje i domena upita u nešifriranom formatu. Na taj način napadač može iz konteksta upita zaključiti koji uređaji proizvođača se nalaze u mreži korisnika. Za neke uređaje je moguće zaključiti i sam tip, a ne samo proizvođača. U sljedećoj tablici možemo vidjeti uređaje i DNS upite koje proizvode:

Tablica 3.1: Primjer DNS upita napravljenih od strane uređaja [22]

Uređaj	**DNS upiti**
Nest Security Camera	nexus.dropcam.com oculus519-vir.dropcam.com pool.ntp.org
Amazon Echo	ash2-accesspoint-a92.ap.spotify.com audio-ec.spotify.com device-metrics-us.amazon.com ntp.amazon.com pindorama.amazon.com softwareupdates.amazon.com

Još jedan način na koji se može zaključiti o trenutnoj aktivnosti korisnika u vlastitoj mreži je i broj paketa koji se šalje u danom trenutku van mreže i njihova periodičnost. Ako se radi o uređaju koji ima mogućnosti virtualnog asistenta moguće je imati uvid u to kada je korisnik imao interakciju s uređajem. Također kod uređaja koji prate spavanje korisnika se broj razmijenjenih paketa drastično poveća kada korisnik spava[22].

Kako najbolje očuvati privatnost korisnika je pitanje s kojim još uvijek mnogi prozivođači imaju problema. To se očituje u ostalim navedenim sigurnosnim propustima u ovom odjeljku. Zakonskim regulativama postiže se veća svijest o bitnosti zaštite podataka te se samim time proizvođači tjeraju na bolje prakse za očuvanjem podataka. Neki od osnovnih načina zaštite korisničkih podataka su:

– šifriranje podataka u svakom aspektu sustava,

- prikupljanje samo nužnih podataka,
- anonimiziranje korisnika,
- bolja kontrola i uvid u podatke za korisnike.

3.2.7. Nesigurni prijenos i pohrana podataka

Podaci koji nisu šifrirani moguće je vrlo lako iščitati. Kriptografijom se postiže sigurnost i privatnost podataka. Kako bi se to postiglo podatke je potrebno šifrirati u svakom koraku njihova nastajanja, prijenosa, obrade i spremanja. Korištenje samih kriptografskih alogritama ne rezultira uvijek i zaštitom podataka. Neki kriptografski algoritmi koriste ključeve nedovoljne dužine i kao takve je potrebno malo vremena da se dešifriraju. Najveći sigurnosni propusti u nedavnoj povijesti povezani su direktno s neadekvatnim kriptografskim algoritmima ili općenitim nedostatkom šifriranja čime su ugroženi osobni podaci i lozinke korisnika[24]. Pozornost se treba posvetiti i kontroli pristupa podacima kako neautorizirani korisnici ne bi mogli pristupiti nedozvoljenim podacima.

Osnovne sigurnosne mjere koje bi se trebale osigurati su:

- šifriranje podataka,
- pravilno korištenje PKI-a (engl. *public key infrastructure*),
- kontrola pristupa podacima,
- korištenje sigurnih protokola za prijenos podataka,
- provjera korištenih kriptografskih algoritama za ranjivosti,
- korištenje dugih kriptografskih ključeva.

3.2.8. Nedostatak mogućnosti upravljanja uređajima

Nemogućnošću upravljanja uređajima ima posljedicu da uređaji u slučaju otkrivenih sigurnosnih propusta ne mogu biti ažurirani, da uređaje nije moguće na jednostavan način otkloniti i uvesti u ekosustav te naknadno proširivati njihove mogućnosti. Zato je jedan od najvažnijih sigurnosnih zadataka u Internet stvari ekosustavima upravljanje uređajima kroz njihov životni ciklus. Ako neautorizirani uređaji budu uvedeni u ekosustav, imat će mogućnost dobivanja pristupa ostalim komponentama ekosustava te nadgledanja mreže i presretanja prometa i informacija.

Zbog heterogenosti trenutnih implementacijskih riješenja jedinstven način upravljanja uređaja je također jedan od problema koji se pojavljuju. Ako imamo više uređaja od kojih svaki zahtijeva svoju platformu i drugačiji način upravljanja, stvara se problem da neki uređaji koji ne zahtijevaju konstantnu pozornost ostanu zaboravljeni, nenadzirani i neažurirani.

Potrebno je imati implementirane načine upravljanja, nadzora i ažuriranja uređaja prisutnih u sustavu. Otkrivanje i identifikacija uređaja je bitan korak u nadgledanju i zaštiti cijelog ekosustava. Heterogenost implementacijskih riješenja uređaja je još uvijek problem s kojim se integratori riješenja susreću, ali kako cijelo područje sazrijeva dolazimo do različitih platformi koje nude integraciju njih svih u jedinstveni ekosustav. Stoga je kod planiranja sustava potrebno uzeti u obzir uređaje kojim je moguće jedinstveno upravljati kako bi se izbjeglo zanemarivanje uređaja.

3.2.9. Nesigurne zadane postavke

Zadane postavke na pametnim uređajima povezane su uz nekoliko primjera. Takav propust se može očitovati kod univerzalno zadanih lozinka, tvrdo kodiranih lozinka ili zadanih postavka programske podrške uređaja. Univerzalne zadane lozinke se pojavljuju kao najednostavniji način prvobitnom pristupu uređaju umjesto nekog drugog načina uspostave uređaja. Takav pristup se mora spriječiti navođenjem upozorenja ili obaveznim postupkom promjene lozinke kod prvobitnog postavljanja uređaja. Tvrdo kodirane lozinke za pristup uređajima je problem koji kod fizičkog ili vanjskog pristupa uređaju može lako dovesti do kompromitacije cijelog sustava te je korištenje takvih lozinka i načina pristupa potrebno izbjegavati. Zadane postavke programske podrške koje mogu dovesti do sigurnosnih propusta je dužnost proizvođača da tijekom testiranja i sigurnosne revizije uoći i onemogući sve nepotrebne i potencijalno nesigurne postavke programske podrške uređaja. To uključuje i sve metode koje su se koristile za testiranje i otklanjanje pogrešaka tijekom razvoja uređaja.

Ovaj sigurnosni propust nije isključivo vezan uz uređaje. Nesigurne zadane postavke se javljaju i na poslužiteljima te ostaloj opremi koja sudjeluje u cijelom lancu komunikacije. Usluge koje se javljaju kao zadane na operativnim sustavima poslužitelja ponekad su i nepotrebne za rad sustava. Takve usluge mogu imati zadane postavke koje dozvoljavaju jednostavan ili nesiguran pristup poslužitelju. Ovakav tip ranjivosti se nadovezuje na propust nesigurnih mrežnih sučelja. Jedan od takvih primjera je konfiguracija vatrozida mreže, koja po zadanim postavkama može dozvoliti nesmetan doljev vanjskog prometa prema lokalnoj mreži.

Spriječavanju sigurnosnih propusta vezanih uz nesigurne zadane postavke se treba pristupiti iz dva smjera. Prvi je od strane korisnika, ako uređaj dolazi sa općenitom zadanom pristupnom loznikom, korisnika se treba obavijestiti da promjeni lozinku. Drugi je sa strane proizvođača da prije nego što se uređaj stavi u upotrebu, ukloni sve zadane postavke vezane uz testnu okolinu i lako pristupanje uređaju poput tvrdo kodiranih lozinki. Kod uspostave poslužitelja potrebno je obratiti pozornost na konfiguraciju mrežnih usluga koje dozvoljavaju pristup i upravljanje samim poslužiteljem, to se odnosi i na sve mrežne uređaje koji se nalaze u lokalnoj mreži uređaja kako bi komunikacija bila sigurna i spriječavala neautorizirani vanjski pristup.

3.2.10. Nedostatak fizičke sigurnosti

Uređaji koji se koriste u Internetu stvari su u nekim slučajevim postavljeni na širokim, raspršenim i nenadziranim područjima poput polja ili šuma. Takvim uređajima je potrebna fizička sigurnost kako bi se spriječili napadi direktnomm pristupu prvobitno uređaju, a zatim i napadi na ostatak sustava. Takvi uređaji postavljeni na otvorenom se nalaze u zaštitnim kučištima te je prvi korak napada otvaranje tog kučišta. Zato je potrebno zaštiti kučišta te implementirati načine otkrivanja neovlaštenog pristupa (engl. *anti-tempering detection*). Ako napadač uspješno fizički pristupi uređaju postoji nekoliko načina pristupa informacijama ili radu uređaja. Informacije se često na takvim uređajima spremaju na memorijske kartice iz kojih je izvlačenje spremljenih informacija moguće ukoliko sam sadržaj nije šifriran. Takvim načinom napada se može izvući lozinke ili privatni ključevi koje uređaj koristi za pristup vanjskim servisima. Na uređajima se također znaju nalaziti pristupni priključci poput USB ili serijskih priključaka. Ako ne postoji način autorizacije pristupnog korisnika moguća je kompromitacija samog rada uređaja. Ti priključci se koriste za testiranja te se kod stavljanja uređaja u upotrebu često ne onesposobe.

Kod takvih fizičkih napada ponekad nije cilj kompromitacija sustava već samo onesposobljavanje uređaja za obavljanjem njhovog zadatka. Ako uređaj obavlja zadatke poput nadziranja prostora pomoću senzora za požar, dima ili pokreta, napad na takav uređaj može fizički naštetiti stvarima poput različitih industrijskih pogona, osiguranih prostora i nanijeti veliku financijsku štetu.

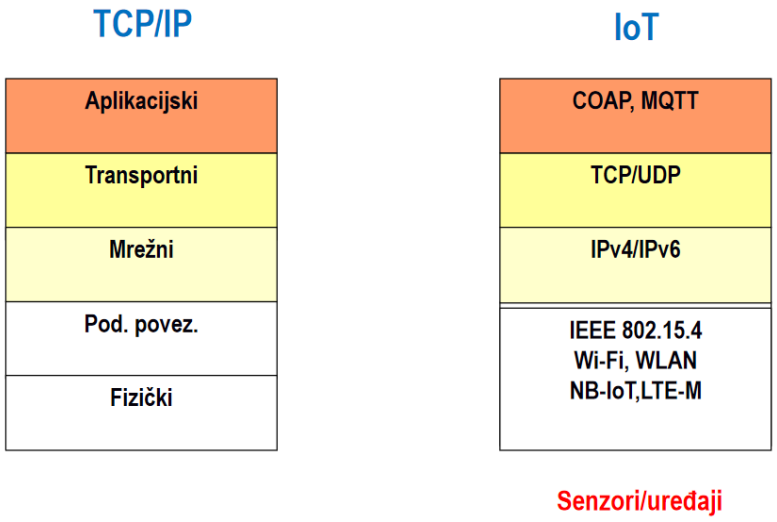
Kako bi se spriječila ili otežao fizički pristup uređajima potrebno je koristiti zaštitna kučišta koja sprječavaju takve napade. Drugi sloj zaštite je korištenje mehanizama za otkrivanje neovlaštenog pristupa uz mogućnost obaviještavanja korisnika o pristupu. Kod samih fizičkih uređaja potrebno je koristiti šifriranje memorije kako bi

se spriječilo čitanje podataka s uređaja. Za pristup radu uređaja uklanjanjanje i onemogućavanje svih nepotrebnih priključaka za pristup je sljedeći korak zaštite. Ako postoji potreban priključak za pristup, pristupanje je potrebno omogućiti samo autoriziranim korisnicima korištenjem kriptografskih ključeva ili lozinkama.

4. Analiza i usporedba protokola

4.1. Protokolni složaj Interneta stvari

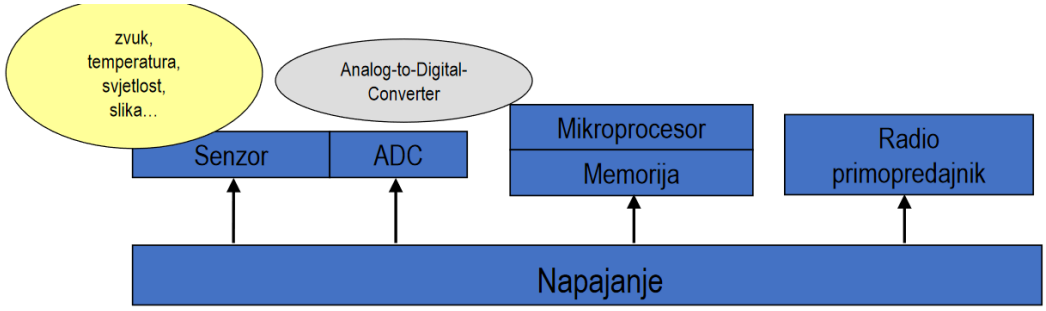
Protokolni složaj Interneta stvari se pobliže temelji na TCP/IP složaju koji podrazumijeva 5 slojeva u svom modelu. Ti slojevi su: fizički sloj, sloj podatkovne poveznice, mrežni, transportni i aplikacijski sloj. Svaki od tih slojeva sadrže različite protokole koji se koriste za komunikaciju na temelju fizičkih, komunikacijskih, identifikacijskih, pristupnih ili semantičkih karakteristika. Na sljedećoj slici su prikazani slojevi prisutni u složaju uz primjere nekih protokola prisutnih u protokolnom složaju Interneta stvari, uz uređaje i senzore navedene kao nulti sloj jer su temelj svakog sustava Interneta stvari.



Slika 4.1: Protokolni složaj Interneta stvari[25]

4.2. Sloj uređaja

Sloj uređaja je bazni sloj u Internetu stvari. Umrežavanjem tih uređaja i korištenjem njihovih senzorskih i aktuatorskih sposobnosti nam omogućava razvoj cjelokupnog sustava Interneta stvari. Uređaji se sastoje od nekoliko komponenti: napajanja, radio primopredajnika, senzora, analogno-digitalnih pretvornika koji dolaze kao zasebni moduli te mikroprocesora, memorije i razvojne pločice kao jedan jedinstveni uređaj. Postoje i već potpuno integrirani uređaji koji sadrže sve prijespomenute module na jednoj razvojnoj pločici. Prikaz modula uređaja nalazi se na sljedećoj slici.



Slika 4.2: Moduli uređaja Interneta stvari[25]

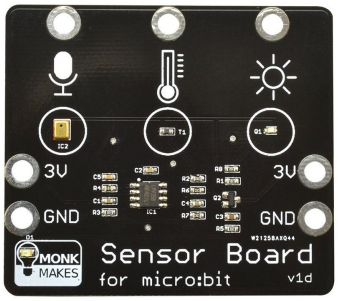
Kod upotrebe Internet stvari uređaja postoji nekoliko zahtjeva koji se razlikuju s obzirom na primjenu. Neki od zahtjeva su: izrazito male dimenzije, mala potrošnja energije, niska cijena i umrežavanje na načelu samoorganizacije. Male dimenzije su potrebne kako bi uređaji djelovali neinvazivno na prostor u kojem se nalaze. Mala potrošnja energije je bitan zahtjev jer dio uređaja je mobilno te nema stalan izvor napajanja već koristi baterije koje nemaju veliki kapacitet ili solarne ćelije čija stopa punjenja nije visoka. Zbog energetske učinkovitosti uređaji imaju ograničenu procesorsku moć te je memorijski kapacitet ograničen. Najveća potrošnja energije se dešava na komunikacijskim modulima čija snaga signala otpada s kvadratom udaljenosti. Svi ti zahtijevi se trebaju uzeti u obzir tijekom planiranja kako bi se mogao utvrditi potreban uređaj za namjenjenu primjenu.

U nastavku će biti opisane senzorske pločice, komunikacijski modul te analizirani pristupni uređaji od kojih su neki potpuno integrirani kao jedna razvojna pločica.

4.2.1. Senzorske pločice

Uloga senzorskih pločica je očitavanje vanjskih fizičkih stvari što je jedna od glavnih mogućnosti sustava Interneta stvari. Senzori prisutni na pločicama omogućuju opaža-

nje različitih vanjskih fizičkih pojava poput: temperature, prisutnosti, pokreta, zvuka, koncentracije plinova, magnetskih polja i protoka vode. Integracija tih pločica s mikrokontrolerima omogućuje procesiranje tih opažanja. Primjer senzorske pločice s mogućnošću očitanja razine buke, temperature i luminacijskog intenziteta je prikazan na sljedećoj slici.



Slika 4.3: Senzorska pločica s mogućnošću očitanja razine buke, temperature i luminacijskog intenziteta[18]

4.2.2. Komunikacijski moduli

Komunikacijski moduli omogućuju uređajima da se umreže u ostatak sustava čime se ostvaruje glavni zahtjev u Internetu stvarima što je povezanost i mogućnost komunikacije. Moduli potrebni za komunikaciju ovise o fizičkom sloju i o sloju podatkovne poveznice. Fizički sloj uvjetuje fizički medij u kojem se podaci prenose. Žičani mediji su: bakrena žica u kojem se radi o elektronima i optički kablovi gdje se informacije prenose fotonima. Bežični mediji su: optički, koji ne koriste kablove već usmjerene laserske snopove koji putuju kroz zrak i radio valove čije različite frekvencije koriste različiti protokoli sloja podatkovne poveznice.

Sloj podatkovne poveznice čine protokoli koji u osnovi opisuju način komunikacije putem fizičkog sloja. Na ovom sloju heterogenost protokola je najprisutnija, posebno kod protokola koji koriste radio valove kao fizički medij. Ta heterogenost se javlja zbog različitih potreba i primjena u sustavima. Tako na ovom sloju imamo različite protokole koji će biti obrađeni u sklopu analize protokola podatkovne poveznice. U nastavku je prikazan komunikacijski modul za ZigBee protokol.

Slika 4.4: ZigBee komunikacijski modul[21]

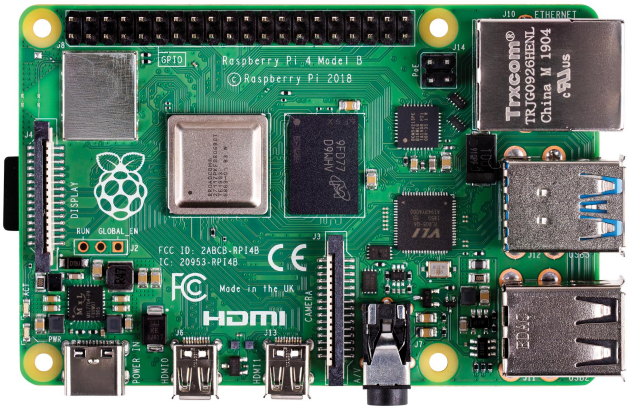
4.2.3. Analiza pristupnih uređaja

4.2.3.1. Raspberry Pi 4 Model B

Raspberry Pi je svojom pojavom na tržištu ponudio malo integrirano računalo za nisku cijenu čime je razvoj Interneta stvari postao pristupačniji za širu zajednicu. Zadnja verzija Pi računala je četvrta s time da sve tri prijašnje verzije su još uvijek u proizvodnji. Razlika između verzija je u procesorskoj snazi, radnoj memoriji, prisutnosti Ethernet i WiFi modula te broju USB i HDMI priključaka. Na Raspberry Pi-u se izvršava GNU/Linux operativni sustav čime se uvelike olakšava razvoj aplikacija i dobiva podrška za već postojeća programska rješenja. Na računalu se nalaze 40 priključnih pinova(engl. *GPIO pins*) koji omogućuju spajanje različitih senzorskih pločica, komunikacijskih modula, napajanja i zaslona čime se postiže visoka modularnost. Raspberry Pi je namjenjen kao stacionaran uređaj zbog njegove relativno visoke potrošnje energije s obzirom na integrirana računala s mikrokontrolerom što zahtjeva konstantan izvor napajanja putem strujnog adaptera. Neke od namjena su kao prilaz za ostale pametne uređaje zbog svoje procesorske snage, kao kontrolni centar sustav za pametan dom korištenjem platformi poput Home Assistanta, a spajanjem modula kamere Raspberry postaje nadzorna kamera.

Raspberry Pi 4 Model B[29] je računalo koje poprima karakteristike stolnog računala. Tako sadrži Broadcom BCM2711, četverojezgreni Cortex-A72 (ARM v8) 64-bit SoC (engl. *System on a chip*), 2, 4 ili 8 gigabajta radne memorije, gigabitni Ethernet priključak, WiFi modul te 2 micro-HDMI priključka koji podržavaju do 4K 60Hz monitore. Te specifikacije dozvoljavaju korištenje RPi4 kao malo stolno računalo, a ne samo kao ugradbeno računalo s nekoliko senzora. Podrška za programske jezike koji se

koriste za razvoj nije ograničen s obzirom na to da uređaj može izvršavati GNU/Linux operativni sustav. Na sljedećoj slici je prikazan Raspberry Pi 4.



Slika 4.5: Raspberry Pi 4 Model B[10]

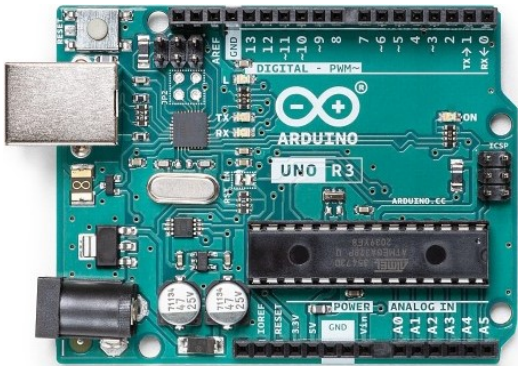
4.2.3.2. Raspberry Pi Pico

Raspberry Pi Pico[30] je malo integrirano računalo s mikrokontrolerom niske cijene. Pico koristi RP2040 mikrokontroler čime se uvelike smanjuje potrošnja energije, ali i procesorska snaga samog računala čija radna frekvencija iznosi 133MHz sa dvije jezgre. Sadrži 264KB SRAM-a te 2MB brze memorije čime je veličina izvršavajućih programa uvelike ograničena. Pico je veličine 21x51mm te tako uz svoju malu potrošnju energije dozvoljava da bude korišten za mobilne potrebe, a sa svojim 26 priključnih pinova dopušta visoku razinu modularnosti. Pristup uređaju se izvodi putem jednog micro-USB 1.1 priključka ili putem UART pinova, ali nema ugrađenih komunikacijskih modula te ako se želi omogućiti pristup mreži potrebno je koristiti zasebne module. Napajanje se provodi putem USB priključka ili putem vanjske baterije spojene na odgovarajuće pinove. Raspberry Pi Pico je ograničen na jednostavne senzorske i aktuatorske primjene zbog svoje ograničene procesorske brzine i kapaciteta pohrane podataka. Podrška za programske jezike koji se koriste za razvoj uređaja je ograničen na MicroPython, CircuitPython, C/C++ te Arduino programski jezik. Uređaj je prikazan na sljedećoj slici.

Slika 4.6: Raspberry Pi Pico[17]

4.2.3.3. Arduino Uno Rev3

Arduino je jedan od najvećih proizvođača malih razvojnih intergriranih računala s mikrokontrolerom koji sadrži različite vrste tih računala koja se razlikuju u dimenzijama, priključcima i cijeni. Arduino Uno Rev3[11] je jedno od tih integriranih računala koje je u svojoj prvoj verziji popularizirало i omogućilo jednostavan i jeftin razvoj za Internet stvari sustave. Shema cijele pločice je sklopovlje otvorenog izvora te je moguće pronači taj isti uređaj od drugih proizvođača. Treća revizija donosi 8 bitni ATmega328P mikrokontroler koji radi na frekvenciji od 16MHz sa 2KB SRAM-a te 32KB programabilne brze memorije. Na pločici se nalazi 20 priključnih pinova od kojih je 14 digitalnih te 6 analognih, uz jedan USB priključak putem kojeg se napaja i jedan zaseban priključak za napajanje. Zbog svoje otvorene i dobro dokumentirane sheme za ovaj uređaj postoji mnoštvo različitih senzorskih pločica i komunikacijskih modula koje je potrebno priključiti ako želimo povezati uređaj na mrežu. Glavna namjena Arduino Una je za brz razvoj jednostavnih Internet stvari rješenja te zbog svoje pristupačnosti je moguće pronači mnoštvo gotovih projekta kako za senzorska tako i za aktuatorska rješenja. Podrška za programske jezike koji se koriste za razvoj uređaja je ograničen na C/C++ te Arduino programski jezik. Na sljedećoj slici je prikazan uređaj.

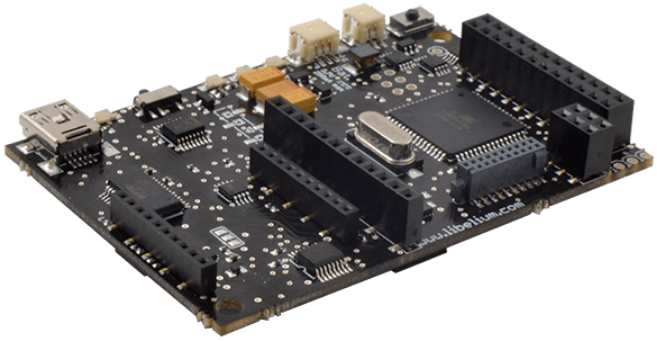


Slika 4.7: Arduino Uno Rev3[11]

4.2.3.4. Libelium Waspmote

Waspmote[20] je bežična senzorska platforma otvorenog koda posebno usmjerena na implementaciju načina rada s malom potrošnjom koja omogućuje čvorovima senzora da budu potpuno autonomni zajedno s prispojenom baterijom. Životni vijek jednog čvora može trajati od 1 do 5 godina, ovisno o radnom ciklusu i korištenim komunikacijskim modulima. Waspmote se temelji na modularnoj arhitekturi gdje je ideja inte-

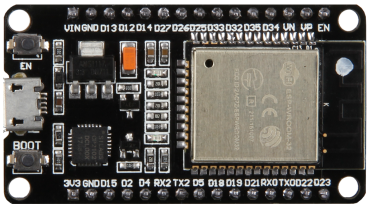
grirati samo module potrebne kako bi se optimizirao rad uređaja. Podržani moduli čine mnoštvo komunikacijskih, podatkovnih modula te senzorskih pločica. Waspmote sadrži 8-bitni ATmega1281 mikrokontroler koji radi na frekvenciji od 14.74MHz, SRAM od 8KB, 128KB programibilne brze memorije te podršku za SD kratice i mini USB priključak. Jedini programski jezik za razvoj je C++. Na sljedećoj slici je prikazan Libelium Waspmote.



Slika 4.8: Libelium Waspmote[20]

4.2.3.5. ESP32

Ravijen od strane Espressif Systema, ESP32[8] je malo integrirano računalo s mikrokontorolerom niske cijene. ESP32 dolazi s integriranim komunikacijskim modulima za WiFi 802.11 b/g/n i Bluetooth s podrškom za BLE(Bluetooth Low Energy). Na pločici se nalazi dvojezgreni Tensilica Xtensa LX6 mikroprocesor s radnom frekvencijom do 240MHz, SRAM od 512KB, 4MB programabilne memorije, jedan micro USB priključak te 34 priključnih pinova. Napajanje se provodi putem USB priključka ili putem vanjske baterije spojene na odgovarajuče pinove. ESP32 je kod primjene najviše zastupljen kod mobilnih primjena zbog svoje niske potrošnje energije i malih dimenzija. Podrška za programske jezike koji se koriste za razvoj uređaja je ograničen na MicroPython, CircuitPython, Lua, C/C++ te Arduino programski jezik. Prikaz ESP32 računala proizvedenog od strane Joy-IT-a je prikazan na sljedećoj slici.



Slika 4.9: Joy-IT NodeMCU-ESP32[12]

4.2.3.6. Pycom FiPy

Pycom FiPy[13] je malo integrirano računalo temeljeno na ESP32 integriranom računalu. Uz sve prije navedene karakteristike i funkcionalnosti ESP32, FiPy sadrži 8MB programabilne memorije i integrirane komunikacijske module za LoRa, Sigfox i LTE-M. Kao i ESP32 FiPy se koristi za pretežito mobilne primjene zbog velikog broja integriranih bežičnih komunikacijskih modula koji dozvoljavaju velike udaljenosti od baznih prilaza što je posebno izraženo ako se koristi komunikacija putem Sigfoxa čiji domet je do 50 kilometara, LoRa čiji domet je do 40 kilometara i LTE-M čiji domet je do 10 km. Na sljedećoj slici je prikazan Pycom FiPy.

Slika 4.10: Pycom FiPy[13]

4.2.4. Usporedba sigurnosnih mehanizama i primjena

Kako bi komunikacija pristupnih uređaja prema vanjskim poslužiteljima bila sigurna potrebno je korištenje kriptografskih algoritama. Ti algoritmi zahtijevaju brzu procesnu snagu što nije slučaj za sve prije navedene uređaje osim Raspberry Pi 4 Model B koji ima četverojezgreni procesor radne frekvenzije od 1.5GHz. Zato kao ispomoć u kriptografskim postupcima na pločicama se također nalazi i zasebni koprocesor za izvođenje kriptografskih algoritama ili podrška za sklopovsko ubrzanje određenih kriptografskih alogoritama. Tako ESP32 i Pycom FiPy nude podršku za sklopovsko ubrzanje SHA, RSA i AES algoritme uz generator nasumičnih brojeva, Libelium Waspmote nudi podršku za kriptografske biblioteke za AES, RSA, MD5 i SHA algoritme iako nije navedena podrška za sklopovsko ubrzanje ili koprocesor. Aruduino Uno Rev3 ne nudi nikakvu posebnu podršku za kriptografske algoritme iako neke verzije Una drugih proizvođača nude podršku za koprocesor za kriptografske algoritme. To je i slučaj sa Raspberry Pi Picom gdje drugi uređaji temeljeni na Pico RP2040 mirkoprocesoru imaju dodatan koprocesor na pločici. Raspberry Pi 4 Model B se približava poziciji stolnog računala te zbog svoje procesorske snage nema potrebe za dodatnim koprocesorima i na njemu se mogu izvoditi svi kriptografski postupci. Zato ako postoji potreba da uređaj samostalno obavlja zadatke i potrebno je osigurati komunikaciju između tog

uređaja i bazne stanice ili poslužitelja najbolje je koristiti uređaje: Raspberry Pi 4 Model B, ESP32 i Pycom FiPy, dok Raspberry Pi Pico i Arduino Uno Rev3 je najbolje koristiti kao integrirano senzorsko računalo koje je dodatno putem priključnih pinova ili USB-a povezano sa snažnijim uređajem.

Primjena svih navedenih uređaja ovisi o njihovim izvorima napajanja, veličini, podršci za komunikacijske module i procesorskoj snazi. Ako gledamo procesorsku snagu i izvor napajanja tu dolazimo do pitanja energetske učinkovitosti uređaja koja ograničava mogućnost upotrebe baterija kao izvora napajanja. Tako će se Raspberry Pi 4 Model B koristiti kao stacionaran pametan uređaj s vanjskim napajanjem, dok ostali navedeni uređaji imaju mogućnost biti baterijski napajani što dozvoljava mobilnu primjenu. Zbog svoje velike procesorske snage Raspberry Pi 4 Model B može djelovati kao poslužitelj i prilaz za ostale pametne uređaje dok su ostali uređaji većinom ograničeni na jednostavne senzorske i aktuatorske primjene. Svi navedeni uređaji imaju podršku za vanjske komunikacijske module te nisu ograničeni na tom području iako neki od uređaja dolaze s već integriranim modulima što dozvoljava brz, jednostavan i jeftin razvoj.

4.3. Fizički sloj i sloj podatkovne poveznice

Fizičkog sloj se definira fizičkim medijem kojem se prenose podaci. Postoje dvije vrste kategorije medija, žičani i bežični na kojima se zatim temelje protokoli podatkovne poveznice. Uloga fizičkog sloja je da definiraju fizički medij koji se koristi u komunikaciji, svojstva tog medija poput frekvencije koja će se koristiti u radiovalnoj komunikaciji, sinkronizaciju, pakete i linijske kodove dok sloj podatkovne poveznice definira strukturu paketa, automate stanja, adresiranje, sinkronizaciju, kontrolu protoka i korekciju grešaka. Na ovim slojevima se nalazi velika heterogenost protokola zbog različitih potreba u sustavima Interneta stvari. Heterogenost protokola je najizraženija u bežičnoj komunikaciji zbog različitih potreba u dometu komunikacije, brzini prijenosa informacija, latenciji i mobilnosti uređaja. Sve ove potrebe su posebno izražene jer upotrebom bežične komunikacije proširujemo mogućnosti primjena uređaja, dok žičane komunikacije uglavnom ograničavamo za potrebe komunikacije prilaza i vanjskih servisa zbog stabilne i brze komunikacije. U nastavku se analiziraju i uspoređuju samo neki od protokola fizičkog sloja i sloja podatkovne poveznice temeljenih na bežičnim tehnologijama.

4.3.1. Analiza protokola

4.3.1.1. IEEE 802.11 WiFi

a

4.3.1.2. Bluetooth Low Energy

Bluetooth Low Energy (BLE) je bežični protokol male snage te je jedan od dva protokola pod Bluetooth nazivom. Drugi protokol je Bluetooth Classic koji se koristi za kontinuiranu komunikaciju velikog skupa podataka na maloj udaljenosti te kao takav je korišten u Internetu stvari, ali za potrebe stacionarnih uređaja sa stalnim izvorom napajanja koji kontinuirano šalju podatke. BLE koristi periodični prijenos manjih podatkovnih paketa te u trenucima kada ne sudjeluje u razmjeni podataka je u stanju mirovanja što uvelike dopinosi smanjenju potrošnje energije. Na taj način se omogućuje razvoj manjih mobilnih uređaja koji mogu biti pokretani duže vrijeme na maloj bateriji.

Na fizičkom sloju BLE koristi ISM (engl. *Industrial, Scientific, and Medical*) radiofrekvencijski pojas na frekvenciji od 2.4GHz. Brzina podatkovnog prijenosa je 1Mbps za verzije 4.2 ili starije, a za verzije 5 i novije može postići do 2Mbps. Udaljenost na kojoj uređaji mogu komunicirati ovisi o preprekama koje se nalaze, vrsti antene, kučištu i orijentaciji uređaja, ali teoretska maksimalna udaljenost je između 100 i 400 metara.

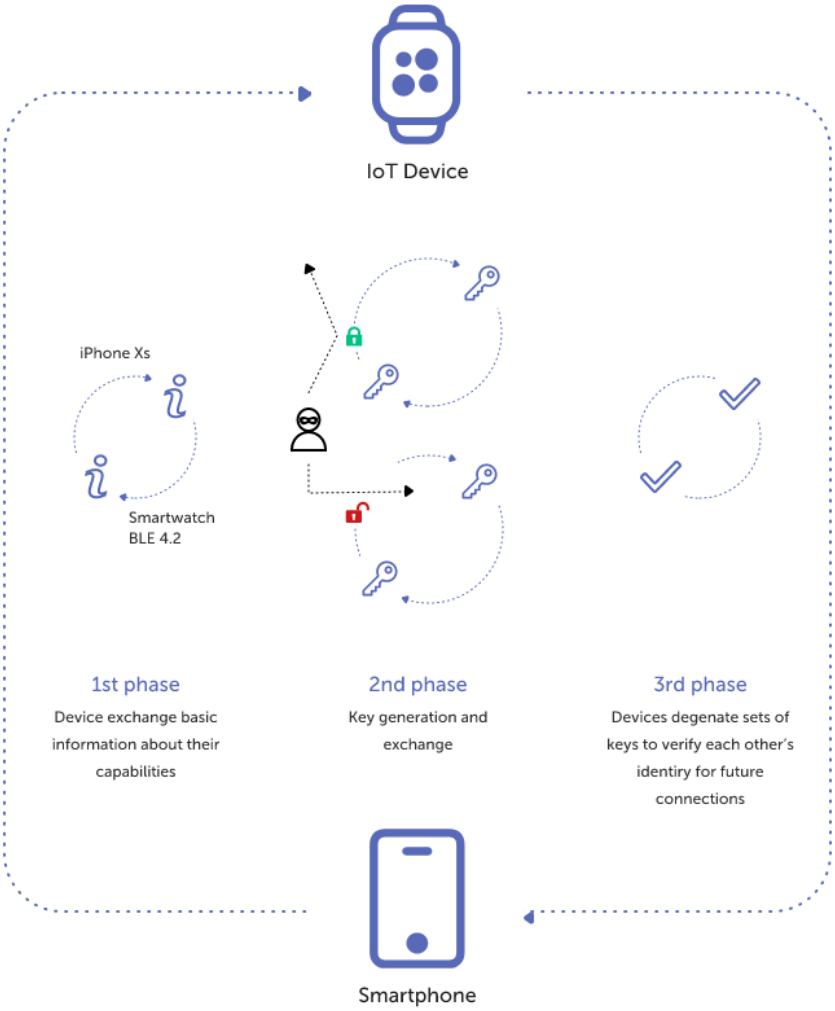
Topologija BLE mreže podrazumijeva dvije vrste uređaja:

Centralni uređaji: imaju veću procesnu snagu i odgovorni su za kontroliranje perifernih uređaja. Na njima se izvode aplikacije posebno izrađene za interakciju s perifernim uređajima. Neki od primjera centralnih uređaja su: pametni telefoni, tableti i računala.

Periferni uređaji: mala integrirana računala koja obnašaju zadaću opažanja koristeći senzore te prikupljene podatke šalju na centralne uređaje za obradu. Neki od primjera perifernih uređaja su: pametni satovi, nosivi medicinski uređaji i industrijski termostati.

Kako bi se mogla odvijati komunikacija između centralnih i perifernih uređaja prvo je potrebno uspostaviti konekciju postupkom koji se naziva uparivanje (engl. *pairing*). Uparivanje se odvija u dvije ili tri faze, tijekom koji uređaji izmjenjuju podatke potrebne za autentifikaciju, poput ključeva i ulazno/izlaznih sposobnosti. Treća faza je

neobavezna te se dešava u slučaju da će uređaji uspostaviti vezu (engl. *bond*). Vezivanje (engl. *bonding*) je proces u kojem uređaji spremaju autentifikacijske podatke koje su izmjenili tijekom prvobitnog uparivanja kako bi se uklonila potreba za ponovnim uparivanje tijekom ponovne uspostave komunikacije. Tijekom prve faze uređaji razmjenjuju informacije o identitetu i sposobnostima uređaja i komunikacija nije šifrirana. Druga faza je posvećena generiranje i izmjeni ključeva te je tijekom ove faze moguć napad *man-in-the-middle* napad gdje napadač može preuzeti kontrolu nad uređajem i podacima koje se prenose. Kod treće faze uparivanja uređaji generiraju set ključeva za autentifikaciju kod budućih uspostava veza. Ti ključevi mogu biti par potpisnih ključeva za razlučivanje konekcije (engl. *Connection Signature Resolving Keys*), koji se koriste za digitalni potpis podataka, te ključevi za razlučivanje identiteta (engl. *Identity Resolving Keys*), koji se koriste za generiranje privatnih MAC adresa i pretraživanje. Kriptografski algoritam koji se koristi za šifriranje prometa je AES (engl. *Advanced Encryption Standard*) s 128 bitnim ključem izveden tijekom postupka uparivanja. Prikaz postupka uparivanja je prikazan na sljedećoj slici.



Slika 4.11: Uparivanje uređaja BLE protokolom[26]

BLE podržava dvije vrste konekcija *Legacy* i *Secure*. Legacy konekcije mogu biti implementirane za verzije 4.0, 4.1 i 4.2. Uređaji razmjenjuju vrijednost privremenog ključa (engl. *Temporary Key*) i koriste tu vrijednost kako bi generirali kratkoročni ključ (engl. *Short Term Key*) koji se zatim koristi za autorizaciju konekcije. BLE Legacy konekcije su nesigurne, ali mogu biti osigurane s određenim metodama uparivanja. Secure konekcije su predstavljane s verzijom 4.2 i nisu kompatibilne sa starijim verzijama protokola. Ove konekcije implementiraju algoritam eliptičke krivulje Diffie-Hellman (ECDH) za generiranje ključeva i donose kompleksniji proces autentifikacije ključima. Na taj način se spriječava napad prisluškivanjem i uređaji mogu biti dodatno osigurani sa određenim metodama uparivanja opisanim u nastavku.

Just Works metoda uparivanja je zadana metoda za većinu BLE mreža. Kod Legacy konekcija vrijednost privremeng ključa tijekom druge faze uparivanja je postavljena na 0 i uređaji generiraju kratkoročni ključ na temelju te vrijednosti. Takva vrsta sprivanja

je jako nesigurna i ne nudi nikakvu vrstu zaštite, već samo način za uspostavu veze. Ova vrsta uparivanja može biti kompleksna i pouzdana za osnovnu sigurnost konekcije kroz sljedeće korake:

1. Korištenjem ECDH kriptografskog algoritma, oba uređaja generiraju privatni i javni par ključeva i izmjenjuju javni ključ.

2. Uređaj koji prima zahtijev za konekcijom generira nasumičnu vrijednost i koristi tu vrijednost kako bi generirao potvrdnu vrijednost. Uređaj šalje obje vrijednosti uređaju koji je inicirao konekciju.

3. Uređaj koji inicira konekciju generira vlastitu potvrdnu vrijednost s nasumičnom vrijednosti koju je primio od drugog uređaja. Uspoređuje vlastitu potvrdnu vrijednost s potvrdnom vrijednosti koju je dobio od drugog uređaja.

4. Ako su vrijednosti identične, uređaji uspostavljaju vezu.

Ova metoda nudi zaštitu od pasivnog prisluškivanja, ali ne i od *man-in-the-middle* napada te se ne preporuča za primjene gdje se razmjenjuju osjetljivi podaci.

Out of Band metoda uparivanja dozvoljava da se određeni podaci tijekom druge faze uparivanja šalju putem nekog drugog bežičnog protokola kako se ključevi ne bi razmijenjivali putem manje sigurnog BLE protokola ili kada uređaji razmjenjuju osjetljive podatke. Krajanja sigurnost ove metode ovisi o protokolu koji se koristi te se na taj način može spriječiti napadi pasivnim prisluškivanjem i *man-in-the-middle* napadi.

Passkey metoda uparivanja koristi korisnike kao dio procesa. Postoje različiti načini implementacije ove metode. Jedan od primjera je da uređaj generira lozinku od šest znamenki, koju tada korisnik treba unijeti na drugom uređaju. Na ovaj način se svaki uređaj ručno verificira od strane korisnika što zahtijeva da uređaji imaju neki oblik unošenja i prikazivanja podataka. Ovim načinom se spriječavaju napadi pasivnim prislušikavnjem i *man-in-the-middle* napadi.

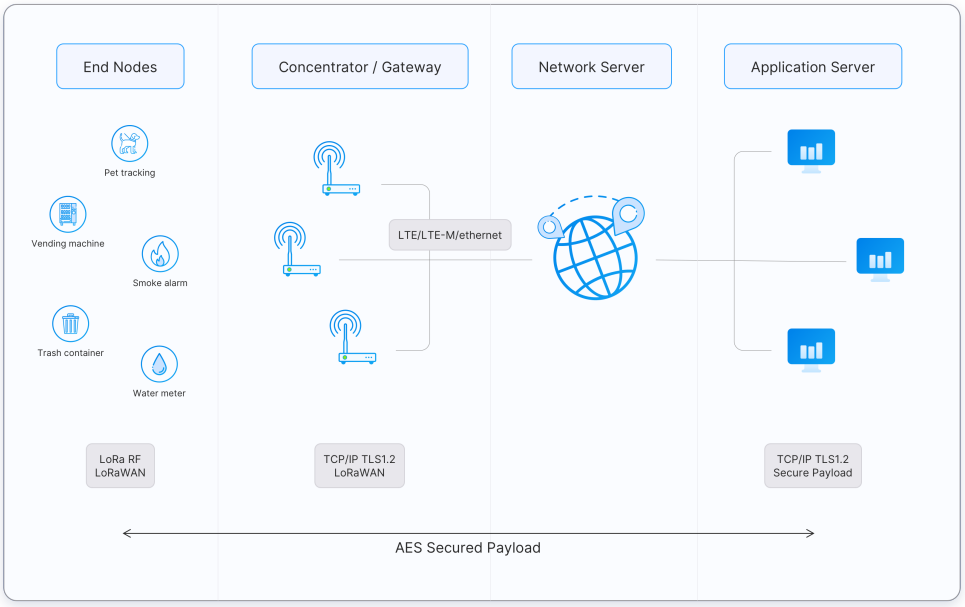
Metoda uparivanja numeričkom usporedbom je dostupna samo za Secure konekcije te također zahtijeva sudjelovanje korisnika. Nakon druge faze uparivanja uređaji koriste nasumične vrijednosti koje su prije razmjenili kako bi generirali šesteroznamenskastu vrijednost koju korisnik treba usporediti na oba uređaja. Ova metoda nudi zađtitu od *man-in-the-middle* napada jer nijedan uređaj se ne može povezati na mrežu bez ručne verifikacije[26].

4.3.1.3. IEEE 802.15.4

IEEE 802.15.4 je standard koji specificira bežične tehnologije prijenosa podataka za uređaje i mreže ograničenih mogućnosti s fokusom na nisku potrošnju energije. Standard specificira fizički sloj i sloj za kontrolu pristupa sredstvu (engl. *Medium Access Control*).

4.3.1.4. LoRaWAN

LoRaWAN (engl. *Long Range Wide Area Network*) je standard za bežičnu komunikaciju koji dovoljava komunikaciju uređaja Interneta stvari preko velikih udaljenosti s minimalnom energetskom potrošnjom. LoRa i LoRaWAN su pojmovi koji se koriste naizmjenično iako definiraju različite slojeve Internet stvari složaja. LoRa definira fizički sloj dok LoRaWAN definira protokol i arhitekturu sustava. LoRa definira različite radiofrekvencijske pojase koji pripadaju ISM pojasevima. U Europi LoRa koristi frekvenicije na pojasu oko 869MHz, dok u Sjevernoj Americi koristi 923MHz čime se javlja nekompatibilnost uređaja prozivedenih za ta dva tržišta. Domet komunikacije ovisi o monogo parametara poput naseljenosti područja u kojem se odvija komunikacija. Za urbana područja domet je oko 5km, predgrađa 10km, a u nenaseljenim područjima može dostići i do 80km. LoRaWAN arhitektura se sastoji od: krajnjih čvorova (uređaja), LoRa prilaza, mrežnog poslužitelja i krajnjih aplikacija. Prikaz topologije LoRaWAN arhitekture je na sljedećoj slici.



Slika 4.12: Topologija LoRaWAN arhitekture[15]

Krajnji čvorovi mogu biti senzori ili aktuatori, često su napajani baterijama i imaju visoku razinu energetske učinkovitosti te tako mogu dugo funkcionirati na jednom punjenju. Postoje 3 kategorije čvorova. Klasa A je najučinkovitija te može primati poruke samo nakon uspješnog slanja poruke s uređaja. Klasa B nadograđuje klasu A i dodaje mogućnost primanja poruka u predodređenim intervalima. Klasa C može primati podatke samo kada ih ne šalje. Uređaji na mreži koriste sljedeće vrste adresa i identifikatora:

DevEUI: Jedinstveni identifikator formata EUI64 (engl. *Extended Unique Identifier*) adrese veličine 64 bita. Usporedivo s MAC adresama za TCP/IP uređaje.

DevAddr: Adresa uređaja veličine 32 bita dodjeljena ili odabrana na mreži. Usporedivo s IP adresama za TCP/IP uređaje.

AppEUI: Aplikacijski identifikator formata EUI64 adrese. Jedinstveno identificira aplikacijskog davatelja usluga uređaja. AppEUI se sprema na krajnji čvor prije nego se izvodi aktivacijski postupak za verzije prije 1.1.

JoinEUI: Identifikator pristupnog poslužitelja formata EUI64 adrese. Jedinstveno identificira pristupnog poslužitelja. JoinEUI se sprema na krajnji čvor prije nego se izvodi aktivacijski postupak za verziju 1.1.

Fport: Identificira vrata aplikacijskog procesa. Usporedivo sa TCP/UDP vratima za TCP/IP uređaje.

LoRa prilazi primaju LoRa poruke od krajnjih uređaja te samo prosljeđuju te podatke na mrežne poslužitelje. Prilazi su povezani na Internet putem drugih protokola poput WiFi-a, Etherneta ili mobilnih mreža.

Mrežni poslužitelji upravljaju cijelom LoRaWAN mrežom. Zadaće poslužitelja su:

- agregiranje svih dolaznih podataka s LoRa prilaza,
- usmjeravanje poruka na aplikacijske poslužitelje,
- konfiguraciju prilaza,
- optimiziranje brzine prijenosa podataka, vremena emitiranja i potrošnje energije na mreži,
- aktivaciju krajnjih uređaja,
- slanje potvrda o primljenim porukama.

Pristupni poslužitelj obrađuju pristupne zahtjeve krajnjih uređaja. Poslužitelj obavlja funkcije spremanja root kriptografskih ključeva, generira ključeve sjednice i prijenosi ključeve sjednice mrežnim i aplikacijskim poslužiteljima. Pristupni poslužitelj je uveden u LoRaWAN mrežu od verzije 1.0.4 i 1.1.

LoRaWAN 1.1 nudi nekoliko razina sigurnosti. Mrežni poslužitelj ne treba imati informaciju o sadržaju poruke koja se usmjeruje, a da nije relevantna za mrežu ili infrastrukturu. Zato postoje dva različita kriptografska 128 bitna ključa koji koriste AES alogritam za šifriranje i 2 ključa za provjeru integriteta poruka kod uređaja kako bi se postigla zaštita podataka na dvije razine. Ključevi korišteni nakon povezivanja uređaja na mrežu su sljedeći:

SNwkSIntKey: Ovo je ključ mrežne sjednice koji koristi uređaj za potvrdu integriteta svake primljene poruke putem *Message Interity Code* (MIC) provjere i za izračun MIC-a za pola odlazne poruke.

FNwkSIntKey: Ovo je ključ mrežne sjednice koji koristi uređaj za izračun MIC-a cijelog ili dijela odlazne poruke.

NwkSEncKey: Ovo je ključ mrežne sjednice koji koristi uređaj za šifriranje i dešifriranje dolaznih i odlaznih poruka MAC naredbi.

AppSKey: Ovo je ključ aplikacijske sjednice koji koriste aplikacija i uređaj za šifriranje i dešifriranje poruka koje izmjenjuju.

Mrežni ključ sjednice (NwkSEncKey) se koristi za komunikaciju između krajnjeg čvora i mrežnog poslužitelja. Ključ potvrđuje integritet svake poruke putem *Message Interity Code* (MIC) provjere. Ta provjera je slična provjeri koristeći kontrolnu sumu uz razliku da onemogućuje neautorizirane promjene sadržaja poruke. Ova provjera se također koristi za mapiranje DevAddr na jedinstvene DevEUI i AppEUI. NwkSEncKey se nakon aktivacije čvora dijeli s mrežom.

Aplikacijski ključ sjednice (AppSKey) se koristi za šifriranje i dešifriranje sadržaja poruka. Sadržaj poruke je šifriran cijelim putem između čvora i aplikacijskog poslužitelja. Ovaj ključ se generira kao i NwkSkey nakon aktivacije čvora, ali samo čvor i aplikacijski poslužitelj imaju taj ključ, što omogučava potpunu tajnost podataka dok ne stigne do aplikacije.

Za aktivaciju čvora i pristupanje mreži kako bi se mogla odvijati komunikacija i kako bi se stvorili kriptografski ključevi se može odviti s dva različita postupka: ABP (engl. *Activation By Personalization*) i OTAA (engl. *Over The Air Activation*).

ABP je najednostavniji način za aktivaciju i pristup LoRa uređaja na mrežu. Dobavljač uređaja od davatelja mrežne usluge otkupi određeni raspon DevAddr adresa i opskrbi svoje uređaje s tim adresama. Nakon što se uređaj upali odmah je spreman za komunikaciju s prilazima. Koraci u postupku aktivacije su:

1. Dobavljač uređaja otkupi mogućnost povezivanja od davatelja mrežnih usluga. AppSKey je generiran unaprijed.

2. Davatelj mrežnih uređaja dostavlja NwkSkey i DevAddr za svaki DevEUI.

3. Prije uporabe uređaja se opskrbljuje uređaje s: NwkSkey, AppSKey i DevAddr

4. Kod prvog korištenja uređaja, nema nikakvog koraka za aktivacijom i pristupa uređaja mreži jer uređaji već mogu komunicirati s mrežom jer imaju sve potrebne informacije.

OTAA je za razliku od ABP postupka kompliciraniji, ali dopušta pristup bilo kojoj mreži u blizini i ne zahtijeva poseban dogov između dobavljača uređaja i davatelja mrežnih usluga. Postupak je različit za verziju 1.1 i ranije verzije, a ovdje ćemo gledati postupak aktivacije za verziju 1.1. Kako bi se sigurnim putem dobavili potrebni ključevi i adresa uređaja postupak koristi dva dodatna kriptografska ključa naziva AppKey i NwkKey koji uz DevEUI trebaju biti spremljeni na uređaju prije postupka aktivacije. To su kriptografski ključevi od 128 bita korišteni za AES kriptografski algoritam. Na pristupnom poslužitelju su spremljeni AppKey, NwkKey i DevEUI. Koraci u postupku aktivacije su:

1. LoRa uređaj šalje Join-request zahtjev potpisan s NwkKey. Zahtjev za pristup mreži sadrži JoinEUI, DevEUI i DevNonce. DevNonce je dvobitni brojač koji počinje s vrijednošću 0 i inkrementira se sa svakim Join-request zahtjevom, a koristi se za sprječavanje napada ponavljanjem. Ovaj zahtijev nije šifriran. Zahtjev LoRa prilazi prosljeđuju na mrežni poslužitelj.

2. Mrežni poslužitelj koristi DNS kako bi doznao IP adresu pristupnog poslužitelja iz JoinEUI polja.

3. Mrežni poslužitelj šalje JoinReq zahtjev na pristupni poslužitelj. Zahtjev sadrži Join-request zahtjev, MAC verziju, DevAddr i druge servisne informacije.

4. Pristupni poslužitelj obrađuje Join-request zahtjev i šalje JoinAns poruku mrežnom poslužitelju. Poruka sadrži Join-accept poruku, NwkSkey, *Serving Network*

session integrity key (SNwkSIntKey), *Forwarding Network session integrity key* (FNwkSIntKey), *Network session encryption key* (NwkSEncKey) i šifrirani AppSKey.

5. Mrežni poslužitelj prosljeđuje primljenu Join-accept poruku krajnjem uređaju. Uređaj izračunava MIC i generira mrežne ključeve sesije i AppSKey. FNwkSIntKey, SNwkSIntKey i NwkSEncKey se izvode iz NwkKey.

6. Mrežni poslužitelj prima odgovor od uređaja te šalje DevEUI i šifriran AppSKey zajedno s porukom aplikacijskom poslužitelju.

7. Aplikacijski poslužitelj prima šifriran AppSKey zajedno s porukom i dešifrira AppSKey koristeći tajni ključ izmjenjen između pristupnog i aplikacijskog poslužitelja. Tada koristi AppSKey za dešifriranje poruke. Ako šifrirani AppSKey nije primljen tada se dovija još jedan korak.

8. Aplikacijski poslužitelj zahtjeva AppSKey izravno od pristupnog poslužitelja slanjem AppSKeyReq zahjeva koji sadrži DevEUI uređaja. AppSKey je šifriran koristeći zajedničku tajnu pristupnog i mrežnog poslužitelja. Pristupni poslužitelj šalje šifrirani AppSKey i DevEUI aplikacijskom poslužitelju u AppSKeyAns poruci. Aplikacijski poslužitelj dešifrira AppSKey i pomoću njega dešifrira poruku uređaja.

9. Nakon aktivacije uređaj ima spremljen DevAddr, FNwkSIntKey, SNwkSIntKey, NwkSEncKey i AppSKey[14].

LoRaWAN mreže se u načinu pristupa i potrebne implementacije dijele u tri skupine: komercijalne gdje mrežu pružaju operateri i naplačuju pristup, javne u koje se može bilo tko uključiti i pružati pristup te privatne koje svatko zasebno može pokrenuti svoju vlastitu privatnu mrežu.

4.3.2. Usporedba sigurnosnih mehanizama i primjena

a

4.4. Mrežni sloj

Mrežni sloj u složaju Interneta stvari omogućava prijenos informacija od prilaza do servisa koji se nalaze u vanjskoj mreži. Glavni način za komunikaciju između mreža je Internet protokol(IP).

4.4.1. Analiza protokola

4.4.1.1. IP

IP definira adresu uređaja kako bi paketi koji se šalju mogli biti usmjereni na taj uređaj. IP se dijeli na IPv4 i IPv6 protokole. Ta podjela postoji zbog ograničenosti IPv4 na 32 bitne adrese koje dozvoljavaju oko 4.2 bilijuna (2^{32}) adresa od kojih su neke rezervirane za posebne potrebe. IPv4 je postao usko grlo na mrežnom sloju, posebice razvitkom Interneta stvari te sve većem broju umreženih mobilnih uređaja. IPv6 donosi 128 bitne adrese koje dozvoljavaju oko $3.4 * 10^{38}$ adresa. Obje verzije protokola sadrže i proširenje pod nazivom IPSec (engl. *Internet Protocol Security*) koji vrši autentifikaciju i šifriranje paketa kako bi se osigurala komunikacija između dva računala preko različitih mreža. Glavna namjena ovog protokola je za uspostavu virtualnih privatnih mreža(VPN) te kao takav je rijetko u uporabi u Internet stvari sustavima već se autentifikacija i šifriranje podataka vrši na aplikacijskom sloju i sloju podatkovne poveznice te ne će biti obrađen u sklopu ovog rada.

4.4.2. Usporedba sigurnosnih mehanizama i primjena

IP ne donosi nikakve sigurnosne mehanizme osim kontrolne sume kod IPv4. Razlog nepostojanja dodatnih mehanizama je postojanje podrške za šifriranjem na slojevima podatkovne poveznice i aplikacijskog sloja te postojanje kontrolne sume na tim slojevima uključujući i transportni sloj. Iako IPv4 sadrži kontrolnu sumu, ta opcija u zaglavlju je izostala iz IPv6 kako bi se smanjila potrebno vrijeme za procesiranjem s obzirom da protokoli viših i nižih slojeva već sadrže tu mogućnost. Nepostojanje sigurnosnih mehanizama kod ovih protokola je najizraženije u takozvanim *IP spoofing* napadima. Taj napad se izvodi promjenom izvorišne adrese kako bi se najčešće izveo DDOS (engl. *Distrubuted denial-of-service*) napad. Napadač mijenja izvorišnu adresu u IP zaglavlju te radi veliki broj zahtijeva na različite servise s odredišnom adresom žrtve koja tada dobiva odgovor od svih servisa na koje su poslani zahtijevi kako bi zagušio i blokirao valjan promet. Obrana od takve vrste napada se najčešće provodi na usmjerivačima analizom prometa kako bi se utvrdili nevažeći paketi.

Primjena IPv4 protokola je još uvijek u velikoj upotrebi usprkos tome što je broj dostupnih adresa davno iscrpljen. Daljnja upotreba protokola je omogućena zbog upotrebe NAT-a (engl. *Network Address Translation*). IPv6 nudi poboljšanja nad IPv4 mogućnošću jedinstvenog adresiranja više uređaja te podrškom da jedan uređaj istovremeno može pripadati više mreža upotrebom više IP adresa. Mogućnošću jedins-

tvenog adresiranja zbog većeg broja adresa jednostavnija je implementacija sustava s ravnopravnim sudionicima (engl. *Peer-to-peer network*).

4.5. Transportni sloj

Transportni sloj je odgovoran za komunikaciju između dva aplikacijska procesa preko mreže. Transportni protokoli definiraju vrata (engl. *port*) koja služe za identifikaciju aplikacijskih procesa na računalima. Najkorišteniji protokoli na transportnom sloju su UDP (engl. *User Data Protocol*) i TCP (engl. *Transmission Control Protocol*) od kojih svaki imaju određena vrata predefinirana za određene protokole aplikacijskog sloja. U nastavku su analizirani i uspoređeni TCP i UDP protokoli.

4.5.1. Analiza protokola

4.5.1.1. TCP

TCP je konekcijsko orijentirani protokol koji za uspostavu konekcije koristi trosmjerno rukovanje. Neka od glavnih svojstva TCP-a su pouzdani prijenos paketa, detekcija pogrešaka, ponovni prijenos kod isteka vremena te kontrola toka i zagušenja. Pouzdani prijenos paketa se postiže korištenjem sekvencijskih brojeva koji identificiraju svaki bajt podataka. Nakon slanja paketa pošiljatelj čeka na potvrdu od primatelja da je primio poslani paket. Detekcija pogrešaka je vezana uz potvrdu primatelja jer se tako može detektirati ako je neki od paketa izgubljen te se ponovno šalje. Pogreške se također detektiraju pomoću kontrolne sume u zaglavlju čime se utvrđuje ispravnost paketa. Ponovnim prijenosom kod isteka vremena se čeka određeno vrijeme na potvrdu primatelja o primljenom paketu te ako dođe do isteka vremena se paket ponovno šalje. Kontrolom toka i zagušenja se upravlja brzinom i veličinom slanja paketa kako bi se pouzdano mogli pošiljati paketi bez preopterećenja primatelja u slučaju male propusnosti mreže ili opterećenja primatelja.

4.5.1.2. UDP

UDP je za razliku od TCP-a beskonekcijski protokol koji ne sadrži svojstva TCP-a za pouzdani prijenos paketa osim detekcije pogrešaka korištenjem kontrolne sume. UDP sadrži četiri polja zaglavlja: izvorišna i odredišna vrata, duljina paketa i kontrolna suma. UDP je namijenjen brzim i vremenski osjetljivim namjenama.

4.5.2. Usporedba sigurnosnih mehanizama i primjena

Svojstva TCP-a omogućava pouzdani prijenos podataka između dvije krajnje točke. Na taj način se osigurava da informacije budu dostavljene bez pogrešaka i u cijelosti. Za razliku UDP nema mehanizme pouzdanog prijenosa podataka što rezultira brzom prijenosu jer ne postoji potreba za dodatnom obradom i kontrolom paketa.

Područja primjene UDP-a je u aplikacijama kojima je brzina prijenosa važnija od cijelovitosti i točnosti informacija poput video poziva, mrežnih igara i reprodukciji video snimaka. Područja primjene TCP-a je u aplikacijama gdje je pouzdanost informacija ključna poput bankovnih sustava, internet trgovini i elektroničkoj pošti.

4.6. Aplikacijski sloj

Aplikacijski sloj je zadnji sloj složaja Interneta stvari preko kojeg se izvodi izravna komunikacija između aplikacija. Protokoli ovog sloja omogućuju postavljanje komunikacijskih pravila između aplikacija kako bi način razmijene podataka bio standardiziran. Aplikacijski sloj sadrži jako veliki broj protokola čija namjena je s obzirom na primjenu jako različita. U nastavku su analizirana i uspoređena tri protokola aplikacijskog sloja koja su najviše zastupljena u Internetu stvari.

4.6.1. Analiza protokola

4.6.1.1. HTTP

HTTP (engl. *Hypertext Transfer Protocol*) je protokol na aplikacijskom sloju za distribuirane, kolaborativne, hipermedijske sustave te koristi TCP kao bazu za komunikaciju između poslužitelja i klijenta. HTTP je u svom začetku bio osmišljen kao protokol za razmjenu hiperteksta, dok je danas zaslužan za razmjenu raznih hipermedijskih sadržaja, tj. teksta, slike, zvuka i videa te kao takav ima najveći udio prometa na Internetu među aplikacijskim protokolima. HTTP koristi URI (engl. *Universal Resource Identifier*) shemu za identificiranje resursa na mrežnoj lokaciji te koristi vrata 80 TCP-a. HTTP djeluje na temelju zahtjeva i odgovora gdje klijent zahtijeva resurs koristeći URI i definirane HTTP metode te na temelju zahtjeva dobiva odgovor od poslužitelja koji sadrži status odgovora, neobavezna polja zaglavlja te zahtjevani resurs u tijelu poruke ukoliko status odgovora poprima format 2XX. Zahtijevi osim tijela poruke također mogu sadržavati neobavezna polja zaglavlja koja daju više informacija vezana uz zahtijev poput zaglavlja koja imaju sigurnosne mehanizme: *Content-MD5* polje koje

služi za provjeru integriteta poruke korištenjem MD5 algoritma za izračunavanje kontrolne sume, *Authorization* polje koje omogućuje autorizaciju korisnika na poslužitelju korištenjem korisničkog imena i lozinke kodirane *Base64* kodnom stranicom ili neke druge vrste autorizacije. HTTP ima nekoliko verzija protokola od kojih su trenutno najzastupljenije HTTP/1.1 i HTTP/2 koje u suštini ne nude prevelike razlike osim veće brzine verzije dva zbog boljeg upravljanja zahtijevima, kompresijom zaglavlja i bolje upotrebe TCP konekcija. Trenutno je u razvoju treća verzija protokola koja kao protokol transportnog sloja koristi UDP i kao zadano donosi šifriranje podataka.

HTTP/S (engl. *Hypertext Transfer Protocol Secure*) je nadogradnja HTTP-a uz korištenje kriptografskog protokola TLS (engl. *Transport Layer Security*) za šifriranje i autentifikaciju. HTTPS kao i HTTP koristi URI shemu za identificiranje resursa na mrežnoj lokaciji, a umjesto vrata 80 koristi vrata 443 TCP-a. TLS podržava razne kriptografske algoritme za šifriranje te digitalne certifikate za autentifikaciju. Verzija TLS-a koja se preporuča za korištenje je TLS 1.3 zbog pronađenih sigurnosnih propusta u prijašnjim verzijama. Postupak kojim se omogućava šifriranje i autentifikacija TLS-om se naziva rukovanje i dolazi nakon uspostava TCP konekcije te se izvodi u sljedećim koracima[19]:

1. **"Client hello" poruka:** Klijent inicira rukovanje slanjem "hello" poruke poslužitelju. Poruka sadržava verzije TLS-a i kriptografske algoritme koje klijent podržava te slučajno generirani niz znakova.

2. **"Server hello" poruka:** Poslužitelj odgovara klijentu sa vlastitom "hello" porukom koja sadrži poslužiteljev digitalni certifikat, odabrani kriptografski algoritam i novi slučajno generirani niz znakova.

3. **Autentifikacija:** Klijent autentificira poslužitelja koristeći certifikacijsko tijelo koje je izdalo certifikat. Na taj način klijent potvrđuje da je poslužitelj onaj koji tvrdi da je i da klijent komunicira sa stvarnim vlasnikom domene.

4. **Tajna koja prethodi glavnoj:** Klijent ponovno šalje novi slučajno generirani niz znakova, takozvana tajna koja prethodi glavnoj. Taj niz znakova je šifriran javnim ključem poslužitelja koji je bio dostavljen u digitalnom certifikatu.

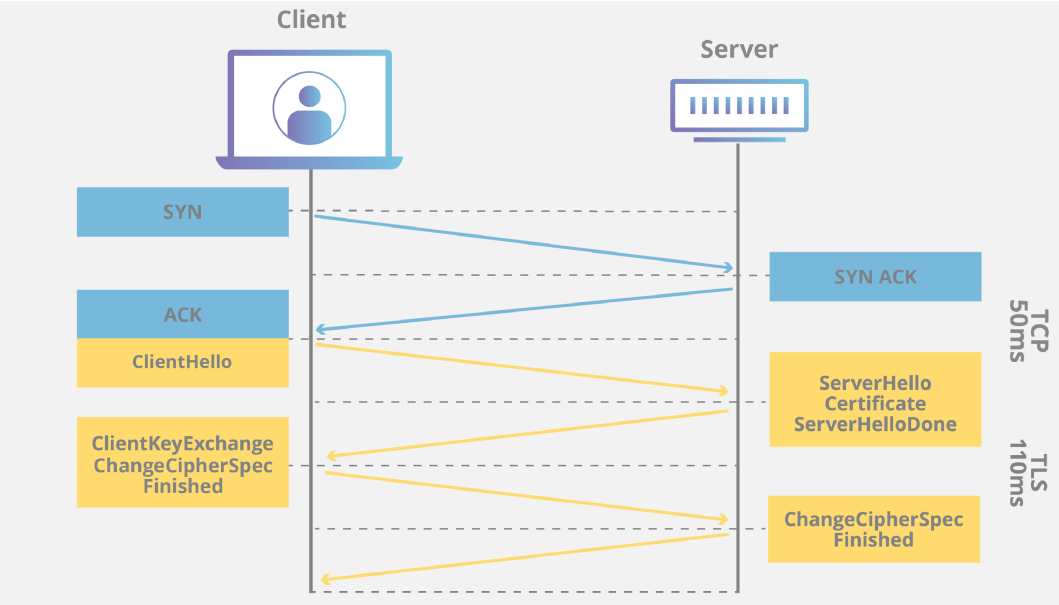
5. **Korištenje privatnog ključa:** Poslužitelj dešifrira primljeni šifrirani niz znakova koristeći vlastiti privatni ključ.

6. **Kreiranje ključa sjednice:** Klijent i poslužitelj kreiraju simetrični ključ sjednice iz prvog klijentskog slučajnog niza znakova, poslužiteljevog slučajnog niza

znakova i tajne koja prethodi glavnoj.

7. **Klijent je spreman:** Klijent šalje "finished" poruku koja je šifrirana sa ključem sjednice.
8. **Poslužitelj je spreman:** Poslužitelj šalje "finished" poruku koja je šifrirana sa ključem sjednice.
9. **Postignuto je sigurno simetrično šifriranje:** Rukovanje je dovršeno i dalje se može izvoditi šifrirana komunikacija korištenjem simetričnog šifriranja.

Na sljedećoj slici je prikazan postupak TCP i TLS rukovanja potreban kako bi se uspostavila HTTP/S sjednica.



Slika 4.13: Prikaz TCP i TLS rukovanja[19]

4.6.1.2. CoAP

CoAP (engl. *Constrained Application Protocol*)[2] je specijalizirani protokol za uređaje ograničenih resursa te kao protokol transportnog sloja koristi UDP na vratima 5683. Protokol je dizajniran za pouzdani prijenos podataka u okolinama male propusnosti i visoke razine zagušenja prometa upotrebom malih zaglavlja paketa i potrebi za maloj procesnoj snazi za obradu zahtjeva. CoAP kao i HTTP djeluje na temelju zahtjeva i dogovora između klijenta i poslužitelja, a koristi URI shemu za identificiranje resursa na mrežnoj lokaciji. Metode koje se koriste u zahtijevima su identične HTTP-u

te se temelje na REST (engl. *Representational State Transfer*) arhitekturi. Metode zahtijeva su definirane kodnim brojem u zaglavlju poruke koje definira i kodni broj statusa odgovora. Kodni broj je veličine 8 bitova. Podržane metode su prikazane u tablici.

Tablica 4.1: Podržane metode CoAP zahtijeva

Metoda	Funkcionalnost	Svojstva
GET	dohvaća resurs na navedenom URI-u	sigurna, idempotentna
POST	stvara priloženi resurs na navedenom URI-u	nije sigurna ni idempotentna
PUT	ažurira ili stvara priloženi resurs na navedenom URI-u	nije sigurna, idempotentna
DELETE	briše resurs na navedenom URI-u	nije sigurna, idempotentna

CoAP podržava četiri vrste poruka:

CON(Confirmable Message): Svaka poruka treba dobiti odgovor ACK ili RESET kao potvrdu.

NON(Non-Confirmable Message): Poruke ne trebaju dobiti potvrdu primitka.

ACK(Acknowledgement Message): Potvrda da je specifična CON poruka zaprimljena.

RESET(Reset Message): Potvrda da je specifična CON ili NON poruka zaprimljena, ali je kontekst poruke nedovoljan da bi se poruka obradila.

CoAP nudi mogućnost promatranja resursa temeljen na pretplati i objavi arhitekturi. Klijent registrira pretplatu na određeni resur korištenjem zaglavlja opcija u kojem postavlja opciju *Observe:0.* Nakon toga se svakim ažuriranjem resursa šalje poruka na pretplačenog klijenta sve dok klijent ne otkaže pretplatu slanjem opcije *Observe:1*. Na ovaj način se smanjuje broj potrebnih razmijenjenih poruka jer se izbjegava periodično slanje zahtjeva klijenta.

Kao što se HTTP osigurava upotrebom TLS-a preko TCP-a, tako CoAP koristi DTLS (engl. *Datagram Transport Layer Security*) za šifriranje i autentifikaciju. DTLS funkcionira na istom principu kao i TLS koji je objašnjen u HTTP odjeljku. CoAP s

ukjučenim DTLS-om za razliku od HTTPS-a koristi UDP kao protokol transportnog sloja na vratima 5684.

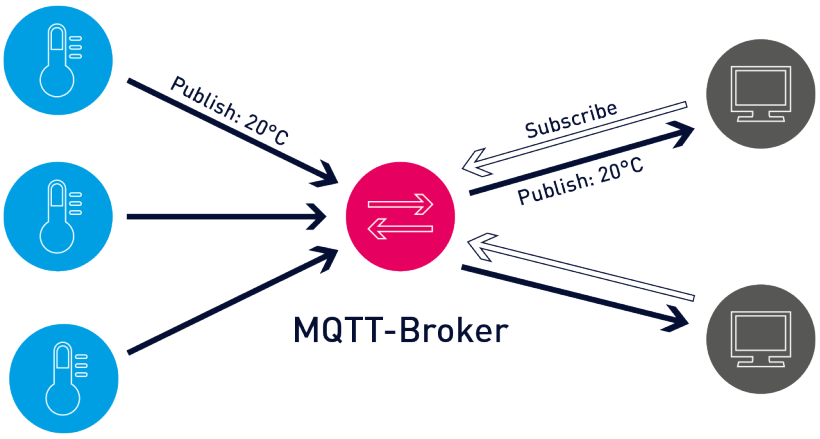
4.6.1.3. MQTT

MQTT (engl. *Message Queuing Telemetry Transport*) je lagani protokol temeljen na porukama, koristi TCP kao protokol transportnog sloja na vratima 1883 te se bazira na topologiji PUSH/SUBSCRIBE. Arhitektura MQTT protokola sadrži dvije vrste sudionika: klijente i posrednike (engl. *broker*).Posrednik je poslužitelj s kojim klijenti komuniciraju putem poruka te posrednik prosljeđuje te poruke na ostale klijente. Na taj način klijenti ne komuniciraju s ostalim klijentima već putem posrednika. Svaki klijent može biti izdavač (engl. *publisher*), pretplatnik (engl. *subscriber*) ili oboje.

MQTT je protokol temeljen na događajima te na taj način nema periodičnog ili stalnog prijenosa podataka čime se smanjuje količina prijenosa. Izdavač šalje poruke jedino kada ima informacije za slanje, a posrednik prosljeđuje poruke pretplatnicima kada primi nove informacije. Još jedan način smanjenja količine prijenosa podataka je korištenjem strogo definiranom, malom konstrukcijom poruka. Svaka poruka sadrži zaglavlje od samo dva bajta, ali može sadržavati i dodatno neobavezno zaglavlje, dok je sadržaj poruke ograničen na 256MB. Tri različite razine kvalitete usluge su dostupne kako bi se moglo odabrati između smanjenja količine i osiguravanja pozudanosti prijenosa podataka. Nulta razina definira slanje poruka pretplatnicima bez potvrde je li poruka primljena, kod prve razine posrednik čeka potvrdu poruke te ako dođe do isteka vremena poruka se ponovno šalje te na taj način pretplatnik može poruku primiti više puta. Druga razina koristi četverostruko rukovanje između klijenta i posrednika kako bi se osiguralo da je poruka primljena i to točno jedan put. Za prvu i drugu razinu poruke se spremaju za klijente koji nisu trenutno dostupni te se ponovno šalju kada klijent postane ponovno dostupan. Na sljedećoj slici je prikazana topologija sudionika MQTT protokola.

Poruke koje izdavači objave se temelje na temama. Teme su strukturirane u hijerarhiju koja teme odvaja znakom "/" kao i kod datotečnih sustava. Primjer takve strukture je **"FER/zgrada-C/kat-7/soba-04/senzor/temperatura"** koja dozvoljava pretplatniku da navede kako želi primati samo informacije o temperaturi sobe četiri sedmog kata FER-ove C zgrade ili da se želi pretplatiti na sve senzore na FER-u koristeći sintaksu "FER/+/+/+/senzor/+". Kod objave prve poruke na temu koja ne postoji ta tema se automatski definira na posredniku bez prethodne konfiguracije.

MQTT podržava 14 vrsta poruka od kojih su osam potvrde, a šest zahtijevi opisani



Slika 4.14: Topologija sudionika MQTT protokola[16]

u nastavku.

PUBLISH: izdavač šalje podatke teme na posrednika. Ako tema ne postoji, ona se stvara na posredniku. Ovisno o definiranoj razini kvalitete usluge posrednik šalje potvrdu o primitku poruke.

SUBSCRIBE/UNSUBSCRIBE: pretvara klijenta u pretplatnika na temu ili uklanja pretplatu na temu. Pretplate mogu biti vezane uz specifičnu temu, sve teme određene razine hijerarhije ili samo određene dijelove određenih razina hijerahije tema. Kao odgovor klijent dobiva potvrdu od posrednika.

PING: Klijent provjerava je li TCP konekcija prema posredniku još uvijek živa. Kao odgovor se dobiva potvrda ukoliko je posrednik dostupan i TCP konekcija živa.

CONNECT/DISCONNECT: Klijent šalje poruku posredniku za otvaranje ili zatvaranje konekcije. Kao odgovor se dobiva potvrda od posrednika o uspostavi konekcije, a kod zatvaranja konekcije se ne šalje potvrda.

Originalan cilj MQTT protokola je bilo smanjenje količine i efikasnost prijenosa podataka kako bi se mogla omogućiti komunikacija putem skupih i nepouzdanih komunikacijskih kanala poput satelitskog prijenosa. Tako kod razvoja protokola sigurnost nije bila primarna briga. Unatoč tome MQTT nudi nekoliko sigurnosnih mehanizama poput korištenje korisničkog imena i lozinke za autorizaciju klijenta kod posrednika. Nedostatak kod implementacije autorizacije je što se korisničko ime i lozinka prenose u nešifriranom tekstualnom formatu. Problem šifriranja i autentifikacije je riješeno korištenjem protokola TLS te se tada protokolu pristupa putem TCP vrata 8883.

4.6.2. Usporedba sigurnosnih mehanizama i primjena

Sva tri navedena protokola nemaju vlastite mehanizme koji bi omogučavali šifriranje podataka i autentifikaciju te za to koriste protokol TLS kao nadogradnju. HTTP i MQTT koriste TLS s TCP-om kao protokol transportnog sloja dok CoAP koristi DTLS koji koristi UDP za protokol transportnog sloja. TLS i DTLS su funkcijski identični protokoli s jedinom razlikom u korištenom transportnog protokolu. HTTP i MQTT također imaju neobaveznu podršku za autorizacijom klijenta korištenjem korisničkog imena i lozinke.

HTTP je u svojoj primjeni puno fleksibilniji zbog mogućnosti prijenosa bilo koje vrste podataka koji uključuju hipertekstualne datoteke, slike, video i audio zapisa te kao takav je najzastupljeniji protokol aplikacijskog sloja na Internetu. Za razliku su MQTT i CoAP protokoli dizajnirani kao lagani protokoli za uređaje i mreže ograničenih resursa. Tako je glavna namjena tih protokola kod praćenja očitanja i jednostavnih događaja pretežito prisutnih u Internetu stvari.

5. Sustav za praćenje tjelesne temperature

5.1. Arhitektura sustava

a

5.2. Korišteni razvojni alati i uređaji

a

5.3. Opis rada sustava

a

5.4. Sigurnosna analiza sustava

a

6. Zaključak

Zaključak.

LITERATURA

[1] The "Only" Coke Machine on the Internet, Jun 1998. URL https://www.cs.cmu.edu/~coke/history_long.txt.

[2] Constrained Application Protocol (CoAP), Mar 2012. URL https://tools.ietf.org/id/draft-ietf-core-coap-03.html#opt. [Online; accessed 17. Jun. 2021].

[3] Overview of the Internet of things ITU-T Y.4000/Y.2060 (06/2012), Jun 2012. URL http://handle.itu.int/11.1002/1000/11559.

[4] Cisco (2014) The Internet of Things Reference Model. - References - Scientific Research Publishing, Jun 2014. URL http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf.

[5] UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA, 2016. URL https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32016R0679&from=HR.

[6] Number of IoT devices 2015-2025 | Statista, Nov 2016. URL https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide.

[7] Owasp top ten 2017, May 2017. URL https://owasp.org/www-project-top-ten/2017.

[8] The Internet of Things with ESP32, Feb 2018. URL http://esp32.net. [Online; accessed 14. Jun. 2021].

[9] Owasp internet of things, 2018. URL https://owasp.org/www-project-internet-of-things/.

[10] Introducing the Raspberry Pi 4 - Raspberry Pi Spy, Jun 2019. URL https://www.raspberrypi-spy.co.uk/2019/06/introducing-the-raspberry-pi-4. [Online; accessed 14. Jun. 2021].

[11] Arduino Uno Rev3 | Arduino Official Store, Jun 2021. URL https://store.arduino.cc/arduino-uno-rev3. [Online; accessed 14. Jun. 2021].

[12] NodeMCU ESP32 - Joy-IT, Jun 2021. URL https://joy-it.net/en/products/SBC-NodeMCU-ESP32. [Online; accessed 14. Jun. 2021].

[13] Fipy - Pycom, Jun 2021. URL https://pycom.io/product/fipy. [Online; accessed 14. Jun. 2021].

[14] End Device Activation, May 2021. URL https://www.thethingsnetwork.org/docs/lorawan/end-device-activation. [Online; accessed 20. Jun. 2021].

[15] LoRaWAN Architecture, Jun 2021. URL https://www.thethingsnetwork.org/docs/lorawan/architecture. [Online; accessed 19. Jun. 2021].

[16] What is MQTT? Definition and Details, Jun 2021. URL https://www.paessler.com/it-explained/mqtt. [Online; accessed 17. Jun. 2021].

[17] Raspberry Pi Pico (Latest & original) buy online at Low Price in India - ElectronicsComp.com, Jun 2021. URL https://www.electronicscomp.com/development-board-programmer/raspberry-pi/raspberry-pi-boards/raspberry-pi-pico-india. [Online; accessed 14. Jun. 2021].

[18] Sensor board for Micro:bit, Jun 2021. URL https://shop.mchobby.be/en/microbit/1593-sensor-board-for-microbit-3232100015937-kitronik.html. [Online; accessed 12. Jun. 2021].

[19] What happens in a TLS handshake? | SSL handshake, Jun 2021. URL https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake. [Online; accessed 16. Jun. 2021].

[20] Waspmote » The sensor platform to develop IoT projects - Libelium, Jun 2021. URL https://www.libelium.com/iot-products/waspmote. [Online; accessed 14. Jun. 2021].

[21] ZigBee module FZB5200, Jun 2021. URL https://www.aliexpress.com/item/32812739871.html. [Online; accessed 12. Jun. 2021].

[22] Noah Apthorpe, Dillon Reisman, i Nick Feamster. A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic. *arXiv*, May 2017. URL https://arxiv.org/abs/1705.06805v1.

[23] Tim Greene. Study: Most enterprise IoT transactions are unencrypted. *Network World*, May 2019. URL https://www.networkworld.com/article/3396647/study-most-enterprise-iot-transactions-are-unencrypted.html.

[24] Jaysson Hollingshead. The 7 Biggest Data Breaches of All Time | InfoSec Insights, Sep 2019. URL https://sectigostore.com/blog/the-7-biggest-data-breaches-of-all-time.

[25] Pavle Skočir Ivana Podnar Žarko, Mario Kušek. Internet stvari, 2. predavanje. Zavod za telekomunikacije, Fakultet elektrotehnike i računarstva, 2020.

[26] Daryna Kacherovska. How Secure Is the BLE Communication Standard? *Dzone*, Aug 2019. URL https://dzone.com/articles/how-secure-is-the-ble-communication-standard.

[27] Bernard Meyer. After analyzing 15 billion passwords, these are the most common phrases people use | CyberNews, May 2021. URL https://cybernews.com/best-password-managers/most-common-passwords.

[28] Mark Patel, Jason Shangkuan, i Christopher Thomas. What's new with the Internet of Things? *McKinsey & Company*, Jan 2018. URL https://www.mckinsey.com/industries/semiconductors/our-insights/whats-new-with-the-internet-of-things.

[29] The Raspberry Pi Foundation. Buy a Raspberry Pi 4 Model B – Raspberry Pi, Jun 2021. URL https://www.raspberrypi.org/products/raspberry-pi-4-model-b. [Online; accessed 14. Jun. 2021].

[30] The Raspberry Pi Foundation. Buy a Raspberry Pi Pico – Raspberry Pi, Jun 2021. URL https://www.raspberrypi.org/products/raspberry-pi-pico. [Online; accessed 14. Jun. 2021].

POPIS SLIKA

POPIS TABLICA

Analiza i usporedba sigurnosnih mehanizama u Internetu stvari

Sažetak

Sažetak na hrvatskom jeziku.

Ključne riječi: Ključne riječi, odvojene zarezima.

Analysis and comparison of IoT security mechanisms

Abstract

Abstract.

Keywords: Keywords.